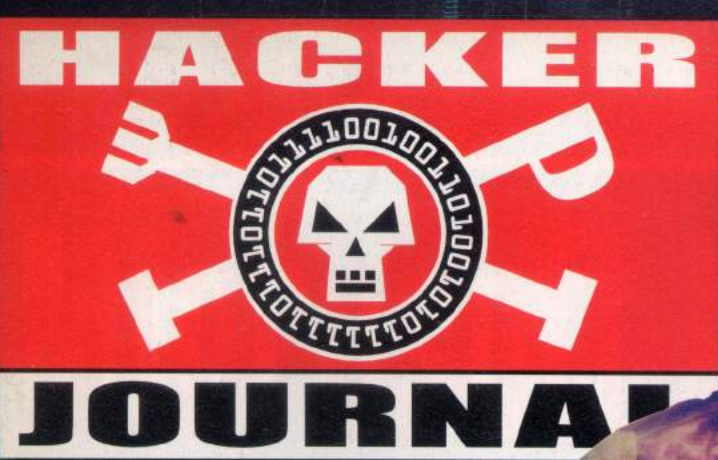


n. 48
www.hackerjournal.it



Abbiamo parlato con il mitico KEVIN MITNICK

2€ NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

Attentato alla libertà:

vogliono mettere fuori legge il P2P



QUATTORDICINALE ANNO 3
8 APRILE 2004 - 22 APRILE 2004
SPED. IN ABB. POST. 70% - MILANO

4ever

Microsoft FINALMENTE CONDANNATA!

Multa di 497 milioni di Euro a Bill Gates

HACKER JOURNAL

Anno 3 – N. 48
8 Aprile 2004 - 22 Aprile 2004

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron
Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Gli articoli contenuti in Hacker Journal hanno scopo prettamente didattico e divulgativo. L'editore declina ogni responsabilita' circa l'uso improprio delle tecniche che vengono descritte al suo interno. L'invio di immagini ne autorizza implicitamente la pubblicazizone gratuita su qualsiasi pubblicazione anche non della 4ever S.r.l.

Copyright 4ever S.r.l.
Tutti i contenuti sono Open Source per l'uso sul Web. Sono riservati e protetti da Copyright per la stampa per evitare che qualche concorrente ci freghi il succo delle nostre menti per farci del business

CLAMOROSO:

Iperbolica multa inflitta a Microsoft dall'antitrust dell'Unione Europea: 497,2 milioni di Euro, la più alta mai chiesta. Giustizia è fatta?

Era ora! Posizione dominante che non permette la libera concorrenza: questo è in sintesi il cappio messo intorno al collo di zio Bill. O paghi, o stringiamo. Oltre a pagare, entro 90 giorni zio Bill dovrà mettere sul mercato una versione di Windows in cui non ci sia più Media Player, ovviamente senza costi aggiuntivi per l'utente.
Entro 120 giorni, soprattutto, Microsoft dovrà fornire ai concorrenti le informazioni per consentire ai programmi di altri di integrarsi al meglio con il sistema operativo montato sui server di fascia bassa. Idem per le applicazioni che verranno realizzate in futuro. Niente da fare per il codice sorgente che è coperto dai diritti sulla proprietà intellettuale e, per averne anche solo dei pezzi, richiederà comunque ai produttori di software l'eventuale acquisto da Microsoft.

La cifra richiesta a Microsoft dall'Unione Europea è la più alta mai imposta per una singola impresa (nel 1991 erano stati chiesti 75 milioni di euro alla Tetra Pack), e a dirla tutta di seguito, ha dello stratosferico: quattrocentonovantasettemilioni e passa di Euro. Eppure è qualcosa come poco meno

LA LEGGE È UGUALE PER TUTTI

L'ACCUSA

Il commissario europeo alla concorrenza Mario Monti: "una concorrenza non distorta comporta risultati migliori per il bene dei consumatori e questo precedente permette di stabilire come procedere in casi simili in futuro". Quanto alla decisione per una multa "proporzionata ed equilibrata" ha detto che "non è stata presa alla leggera ma è seguita a cinque anni di indagini, a lunghe discussioni con i nostri esperti e a consultazioni con i 15 stati membri".



LA REAZIONE

Microsoft si appellerà contro la decisione dell'Antitrust (ma a questo proposito Monti si è detto "sicuro di vincere anche il ricorso"). "Sebbene riteniamo che la decisione di oggi sia sbagliata - ha detto il CEO di Microsoft, Ballmer - continueremo a collaborare e cooperare con i governi e l'industria europei per affrontare temi condivisi, come l'interoperabilità, la sicurezza, la privacy, lo spam e la tutela dei minori in rete".

LA BATTAGLIA DEI DIECI ANNI

È dal 1994 che la commissione europea sta alle calcagna di Microsoft. Tutto è iniziato da quando la UE accusò Microsoft di usare i suoi brevetti in modo illecito, per bloccare la concorrenza. Microsoft promise qualche cambiamento della strategia commerciale. Più tardi, nel 1997, zio Bill viene nuovamente accusato di non rispettare gli accordi del 1994. Si procede alla firma di un altro compromesso. Nel 1998 Sun Microsystem denuncia Microsoft

Microsoft CONDANNATA!



dell'1,6% del volume d'affari Microsoft nel mondo. Come dire noccioline, un sassolino nella scarpa, per una società che ha dichiarato di avere in cassaforte 45 miliardi di Euro, solo come liquidità. (Sigh...) Ci vorrebbero altre cento cause perse del genere per dare veramente fastidio al gigante di Redmond.

Il buchino nella diga

È il principio che conta. Solamente una diecina di anni fa i concorrenti di Bill Gates erano potenzialmente tutti, milioni di sviluppatori sparsi nel mondo. Quanti sono oggi? Tre, forse quattro.
Eh no, signori. Non possiamo continuare ad acquistare PC con preinstallato un unico sistema operativo, senza che si possa realmente decidere come si vuole che funzioni il proprio computer. In pochi hanno provato a chiedere la disinstallazione e il rimborso, passando per alieni in un mondo uniformemente assuefatto e dovendo fare i salti mortali tra le articoli e licenze (http://attivissimo.homelinux.net/rimborso_windows/istruzioni.htm). Forse, ora, una piccola crepa al sistema è stata messa. Un forellino nella diga è stato fatto e non c'è ditino di zio Bill che possa chiuderlo... la dirompente forza dell'acqua compierà fino in fondo il suo lavoro?

Non tutto il male...

Microsoft, nella difesa e nei commenti del dopo-multa, ha fatto notare che un sistema operativo senza Windows media player non permetterà agli utenti di vedere una quantità impressionante di siti su Internet, basati sul file multimediali in formato adatto al Media Player. E tra questi, citiamo il grande capo Microsoft Steve Ballmer, "anche il sito del parlamento italiano". Ecco, appunto. Che fine ha fatto la 'svolta Linux' che qualche tempo fa si era prospettata anche alla Commissione Europea?



Il primo passo è stato un buon passo, ma vogliamo sperare che sia solo l'inizio. In linea di principio le premesse ci sono tutte. Basta con gli strapoteri dominanti, forza con la condivisione. Libertà digitale vuole dire anche questo. ■

NON ILLUDIAMOCI

Qualche tempo fa Microsoft era stata condannata dall'antitrust degli Stati Uniti ad essere smembrata e a pagare multe salatissime. Una serie di ricorsi e di patteggiamenti hanno evitato lo smembramento e ridotto (notevolmente) le multe. Microsoft ha già annunciato ricorso alla multa commissionata dall'Unione Europea e già sono iniziate le pressioni internazionali. Personaggi di spicco del governo e del parlamento americano hanno criticato la sentenza definendola "un errore". Staremo a vedere...



TUTTI CONTRO MICROSOFT

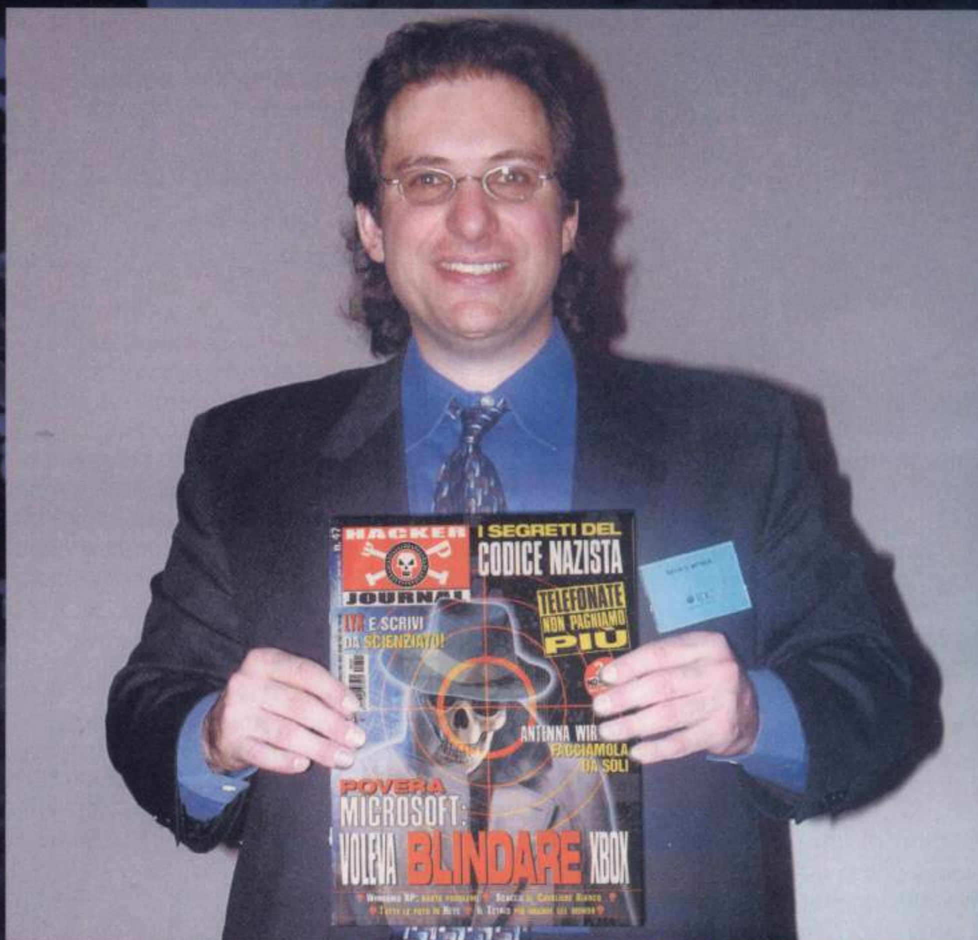
In Giappone le autorità stanno indagando per capire se Microsoft ha infranto le norme sui monopoli, RealNetworks ha iniziato una causa sostenendo che Windows Media Player incluso in Windows è una forma evidente di monopolio, un milione di abitanti del Minnesota hanno costretto lo stato americano a una causa legale verso Microsoft per avere dovuto usufruire a prezzo maggiorato di servizi della società di Bill, tra il 1994 e il 2001. Altre grandi società europee stanno pensando come usare l'iniziativa dell'Unione Europea per scardinare il colosso americano su altri fronti.



all'antitrust europeo per abuso di posizione dominante, per non pubblicare informazioni che consentano a Windows di dialogare con server concorrenti. È all'inizio del 2000 che l'antitrust ufficializza l'inchiesta contro Microsoft per violazioni al mercato che riguardano in particolare Windows 2000. È partito l'attacco definitivo. Nel 2003 un ultimatum della commissione europea con proposta di multa per un miliardo di Euro, per violazione di posizione dominante. E finalmente arriva il 2004: si prova a negoziare un compromesso ma le trattative falliscono il 17 marzo, quando Microsoft rifiuta di prendere impegni per il futuro, in particolare per rendere accessibile alla concorrenza Windows, e il suo successore in sviluppo, per quanto riguarda l'inclusione di prodotti alternativi a Media Player. Come è finita lo sappiamo.

IL CONDOR

L'hacker più famoso del mondo ha fatto tappa a Milano, e abbiamo avuto occasione di incontrarlo!



A vederlo non sembra proprio il re degli ingegneri sociali: completo business, capello all'indietro, pancetta incipiente. Ma forse il suo segreto è proprio quello, apparire così inoffensivo che dieci minuti dopo è padrone di tutti i segreti di chi gli si trova davanti. È questa l'arte che da giovanissimo lo ha reso padrone delle reti telefoniche delle due coste americane, oppure gli ha consentito di farsi mandare da personale Motorola codice sorgente superconfidenziale di Motorola stessa. È anche la stessa arte che lo ha mandato nei guai e, nel processo che ha subito, lo ha fatto condannare, tra l'altro, a stare lontano per anni da qualsiasi tipo di apparecchio telematico.

Ciononostante Kevin Mitnick è riuscito a scrivere un libro, The Art of Deception, ed è venuto a presentarlo anche a Milano, al Marriott Hotel, nel corso della Security Conference 2004. Per un'ora ha intrattenuto da cabarettista consumato centinaia di persone, raccontando le sue imprese ma anche spiegando perché l'ingegneria sociale è la forma di attacco più efficace contro un'organizzazione non preparata.

"Kevin qual è il tuo sistema operativo desktop preferito?"

"Non pensate che sia Windows solo perché ho una presentazione con PowerPoint! Preferisco FreeBSD per le sue qualità di sistema sicuro, anche se poi sul lavoro uso spessissimo Linux o altri derivati di Unix"

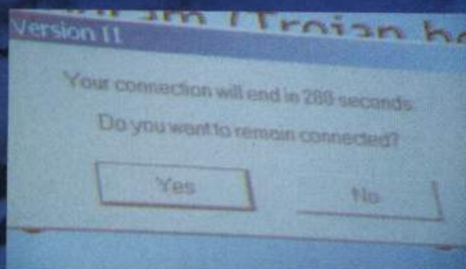
Ecco alcune delle numerose gemme della presentazione di Kevin. La traduzione è molto libera, ma assolutamente fedele al senso.

"La gente pensa che acquistando un bel firewall costoso risolve i propri problemi di sicurezza, *ma nella mia*

VOLA ANCORA!

esperienza sono le persone l'anello più debole di qualsiasi catena e sistema di difesa. Qualsiasi persona all'interno di una organizzazione è vittima potenziale di un attacco di ingegneria sociale. Le armi dell'ingegnere sociale sono curiosità, abilità psicologica, capacità di programmare e improvvisare al tempo stesso. Attaccare in questo modo è più semplice, costa meno, i bersagli sono innumerevoli, c'è sempre un anello più debole degli altri, si corrono pochi o nessun rischio".

"Una delle maggiori fonti di informazioni sono i siti Web delle aziende. Ma non bisogna trascurare niente. Altra risorsa importantissima: gli elenchi del telefono. Per non parlare dei bidoni della spazzatura. Una volta, insieme a un amico, abbiamo frugato nella spazzatura del centro dati di un'azienda. I centri dati producono la spazzatura migliore! In fondo al sacco abbiamo trovato un mucchio di striscioline di carta. Ci siamo messi con pazienza a ricomporre il puzzle. Alla fine avevamo in mano la lista completa di user e password dell'azienda! Morale: mai stracciare le informazioni più importanti. Meglio non stamparle, oppure bruciarle".



▲ A un certo punto della sua presentazione alla Security Conference perfino il computer di Kevin è stato "attaccato"!

DAL NORAD A SHIMOMURA

La prima violazione di sistema effettuata da Kevin Mitnick risale al 1982: entrò nel NORAD, il comando militare nordamericano, e ispirò la sceneggiatura del film War Games. Nel 1992 si diede alla clandestinità dopo avere attaccato il sistema di voice mail di Pacific Bell e, con lo pseudonimo di Condor, ha colpito Motorola, Nokia, Fujitsu, Novell, NEC, Sun e altri, causando danni per una stima di 80 milioni di dollari. È stato arrestato nel 1995 dopo essere entrato nel computer dell'esperto di sicurezza Tsutomu Shimomura, che gli aveva lanciato una sfida. Ha fatto cinque anni di carcere e oggi lavora come consulente di sicurezza.

"Una prestigiosa società di analisi finanziaria del Colorado ha addestrato per tre mesi tutti i suoi dipendenti sulle questioni di sicurezza.
Da consulente in sicurezza ho effettuato un test di penetrazione via ingegneria sociale. Dieci telefonate e sono entrato nel sistema".

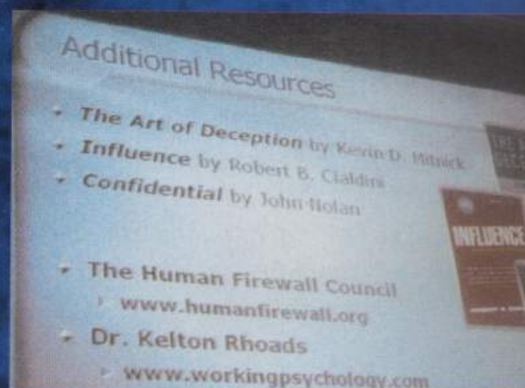
"Alla stazione della metropolitana di Waterloo a Londra nove persone su dieci ti dicono la password del loro computer se gli regali una penna. Pochi anni fa erano quattro su dieci".

"Se abbiamo un problema su Windows, scarichiamo un update. Ma contro l'ingegneria sociale non c'è update da scaricare!"

"Qual è l'attacco migliore? Quello contro l'help desk. Perché? Perché sono lì per aiutare, no? Troviamo il nome di qualcuno nell'organizzazione; troviamo il suo numero di sicurezza sociale [simile al nostro codice fiscale. N.d.B.], o il suo interno, e usiamo queste informazioni per risalire ad altre informazioni e così via".

"E le guardie di sorveglianza? Tempo fa ho chiamato in un laboratorio universitario di notte. C'era solo la sicurezza. 'Per favore, sono del laboratorio, ho bisogno urgente di un'informazione dentro uno dei computer e non posso muovermi da casa'. 'Ma certo, che posso fare?' Vada al secondo piano, si sieda al computer e digiti quello che le dico [per autenticarsi come root e avere il dominio del sistema. N.d.B.]. Alla guardia ho fatto anche stampare sulla stampante del laboratorio un log delle cose fatte, perché rimanesse la prova dell'hack".

"Oggi tengo corsi di sensibilizzazione di ingegneria sociale. Uno degli esercizi che assegno è questo: nella pausa



pranzo, ottenere tutti i dati di carta di credito del primo sconosciuto che si incontra, e sapere anche quanto guadagna. Per esempio, mentre si è a pranzo, si estrae la nostra carta e si dice 'Ma è vero che hanno cambiato l'ologramma? Me lo ha detto un collega…'. Quasi certamente la vittima estrae la sua, di carta…" [I più bravi cominciano dalla coda alla cassa, probabilmente. N.d.B.]

Non potevamo lasciarlo andare senza mettergli in mano una copia del nostro Journal preferito!

Barg the Gnoll
gnoll@hackerjournal.it

CONVOCATO DALLA POLIZIA POSTALE

Giorni indietro sono stato convocato dalla Polizia Postale, e già lì mi si è ghiacciato il sangue... non potevo minimamente immaginare per che cosa, anche perché dovete sapere che io al PC ci faccio giochi e vado un po' in Internet per fare delle sane chattate e scaricare qualche immagine per i desktop: insomma cosette, niente di particolare e/o illegale... insomma tornando al sodo, sono andato di corsa al comando della P.P. che mi ha fatto una domanda strana : lei conosce questa signora ? E mi hanno detto il nome... Io ho risposto la verità e cioè NO, poi mi hanno detto dove abita e cioè a un centinaio di km da me. Poi mi hanno chiesto altri cinque nomi a me sempre sconosciuti e sempre più lontani... Io a questo punto ho chiesto il perché di queste domande e loro mi hanno risposto perché io e queste altre cinque persone un mese fa circa siamo entrati nella posta di questa signora, avvocato, che ha sporto denuncia, gli abbiamo scaricato la posta e cancellata. Dai tabulati che mi hanno fatto visionare ho visto il mio numero di telefono di casa, la mia connessione e il nome della mia e-mail da dove mi connetto. Aiutatemi... come può essere successo? Io veramente non ho fatto queste cose e avere dei problemi con la legge per non aver commesso niente mi gira proprio i marroni. Un saluto e un ringraziamento a chi mi può aiutare a scoprire questo arcano.

Marlboro70

Caro Marlboro70

dalle tue descrizioni e in quelle che ci riferisci della polizia postale ci sono pochi elementi per capire cosa sia realmente successo. Riassumiamo: un bel giorno ci accorgiamo che qualcuno (?) ha scaricato la nostra posta e poi l'ha cancellata. Un collega di lavoro inesperto o inaffidabile che per sbaglio ha usato il nostro computer? Un semplicissimo virus che ha fatto uno dei tanti danni possibili al nostro PC? Quando e come è avvenuto? Supponiamo, comunque, che dopo la nostra denuncia qualche esperto sia già venuto sul luogo del misfatto, e abbia accertato che non è stato il collega e nemmeno un nostro sbaglio di apertura di una email contenente un virus cattivo. Supponiamo quindi che sia stato accertato, come non abbiamo elementi per saperlo, che sia stato qualcuno 'dall'esterno' che aveva tutti i privilegi di accesso al nostro PC. Bene, con tutti buchi di Windows e prodotti affini può capitare (ma è una vera sfortuna, se siamo utenti normali) soprattutto se non abbiamo installato un firewall software e un antivirus aggiornato. Dopodiché vediamo che sul tabulato compaiono il nostro numero di casa, la connessione e la nostra email: ma queste sono le normali informazioni che qualunque provider deve tenere, e con le nuove leggi per parecchio tempo, anche per tutte le nostre connessioni. Quindi, se sono risaliti a noi, è perché il nostro IP che ci è stato assegnato dinamicamente in un certo momento di un certo giorno è, in qualche modo, arrivato sul computer vittima del reato. Ma anche questo può dipendere da un sacco di cose: un trojan sul nostro computer che ha scandagliato indirizzi IP casuali fino a trovarne uno sprotetto e quindi gli ha installato a sua volta un virus o un worm, che a fatto i suoi danni e poi, probabilmente, si è diffuso ancora. O magari un IP generato a caso per coprire quello vero da cui è partito l'attacco e, sfortuna vuole, coincidente con il nostro in quel dato momento. Insomma, l'unica cosa è stare tranquilli. Se non abbiamo fatto nulla, risulterà evidente dall'approfondimento delle indagini. Che, per seguire una classica strada che nulla deve lasciare al caso, cominciano con una altrettanto classica convocazione di tutti quelli che sono in qualche modo 'testimoni'. Anche se per la complessità dei sistemi tecnologici attuali possono benissimo non esserlo veramente. Un'idea di come raffinate e facili possono essere le tecniche di diffusione di questi "virus" te la puoi fare leggendo l'articolo sul 'phishing scam' che troverai su questo stesso numero. Ciao!

POLIZIA di Stato

[H]ome > Polizia Postale e delle Comunicazioni > Consigli virus | Dipartimento della P.S. | Ministero dell'Interno

[P]ersonalizza

Per il cittadino: Concorsi, Denunce, Passaporto, Moduli, Stranieri, Consigli, Per i più piccoli, Faq

Dove siamo: Le Questure, Uffici di polizia

On line: News, Interventi, Comunicati stampa, Dati statistici, Documentazione, Legislazione, Link

Banche dati: Latitanti, Bambini scomparsi, Auto rubate, Banconote false, Documenti smarriti, Oggetti rubati, Armi

Per gli operatori P. di S.

Indietro

Polizia Postale e delle Comunicazioni

Proteggersi dai virus: alcuni consigli utili

Il timore di infezione da virus informatico sembra essere in aumento tra gli utenti della telematica. Proponiamo una lista di suggerimenti utili per ridurre i rischi di infezione.

1. Fate dei regolari backup dei dati più importanti;
2. Usate un software di protezione dai virus. Questo significa tre cose: caricarlo come primo programma in esecuzione, controllare ogni giorno se vi sono aggiornamenti sui virus e infine fare uno scan dei file del proprio computer periodicamente;
3. Usate un Firewall come un «gatekeeper» tra il vostro computer e la rete Internet. I Firewall sono essenziali per coloro che hanno una connessione ADSL o via cavo a Internet ma sono preziosi anche per chi utilizza la connessione telefonica;
4. Non tenete il computer allacciato alla rete quando non lo usate. E' consigliato piuttosto disconnettere il computer, se necessario, anche fisicamente.
5. Non aprite gli allegati delle e-mail provenienti da sconosciuti e verificate prima il nome dei mittenti e il soggetto;
6. Siate sospettosi anche di ogni allegato inaspettato inviatovi da chi conoscete poiché esso può essere stato spedito senza che la persona ne sia a conoscenza da una macchina infettata;
7. Scaricate regolarmente i «security patches» (modifiche per incrementare la sicurezza dei software) dal vostro fornitore di software.

indietro...

Ci comunicate che... | [C]erca | Rassegna stampa | Chi siamo | Download

www.poliziadistato.it

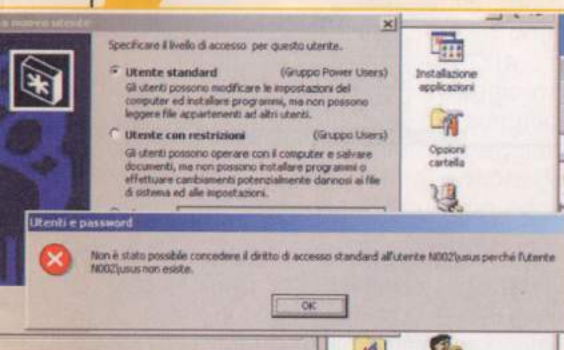
© Copyright 2001 - 2003, Polizia di Stato. Tutti i diritti riservati.

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

WINDOZE, UNO

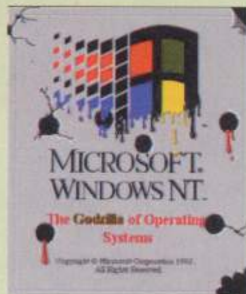
Salve a tutti.
Vi invio, per la serie "messaggi intelligenti", un messaggio di errore di Win2000.
N.B.: Come può non esistere un utente del quale sto cercando di modificare i privilegi di accesso?

Caino79



WINDOZE, DUE

Compariamo il noto sistema operativo con un virus per determinare una volta per tutte se anche Windows è un virus. Ecco cosa fanno i VERI virus: Si replicano velocemente. Ok, lo fa anche Windows.



I virus usano molte risorse del sistema e rallentano il computer. Ok, lo fa anche Windows.
I Virus, a volte rovinano il disco fisso. Ok, lo fa anche Windows. I Virus rendono, occasionalmente, lento il computer (Vedi punto 2) e l'utente acquisterà altro hardware. Ok, lo fa anche Windows. Fino ad ora, sembra che Windows Sia un Virus, ma ci sono fondamentali differenze. I virus sono programmi ben supportati dagli autori, girano su tutti i computer, il loro codice è veloce, compatto ed efficiente e tendono a diventare più sofisticati con il tempo. Quindi, Windows NON è un virus!

CzlineBoyz

TI PIAZZO L'ADSL

Gentile redazione di hj, sono un lettore della vs rivista e vi voglio raccontare quanto stia a cuore a Telecom la sicurezza dei suoi utenti. Qualche giorno fa nell'ufficio dove lavoro, ha chiamato un tecnico del servizio di sicurezza internet di Telecom italia, il quale mi avvisava che chi, come la mia società, utilizza per l'accesso a internet un collegamento ISDN, corre un grave pericolo in quanto durante la navigazione alcuni software maligni a nostra insaputa, deviano il collegamento a numeri telefonici con tariffazione maggiorata e con conseguente addebito in bolletta. Il bravo tecnico, oltre a mettere in guardia me e la mia società, ci propone una soluzione al problema; "...Telecom Italia vi mette a disposizione una linea internet protetta e cioè il passaggio a un abbonamento ADSL smart time con soli 7 al mese di canone fisso per un costo di collegamento di circa 2 l'ora, più una casella di posta elettronica di 30 MB + 3 alias, senza costi di attivazione, così potrete navigare in tutta sicurezza...". Dopo averlo ringraziato per avermi messo in guardia sul pericolo che incombeva sulla mia società, ho subito stipulato un abbonamento ADSL. Smart time. Grazie Telecom. (...ma avrò fatto bene??)

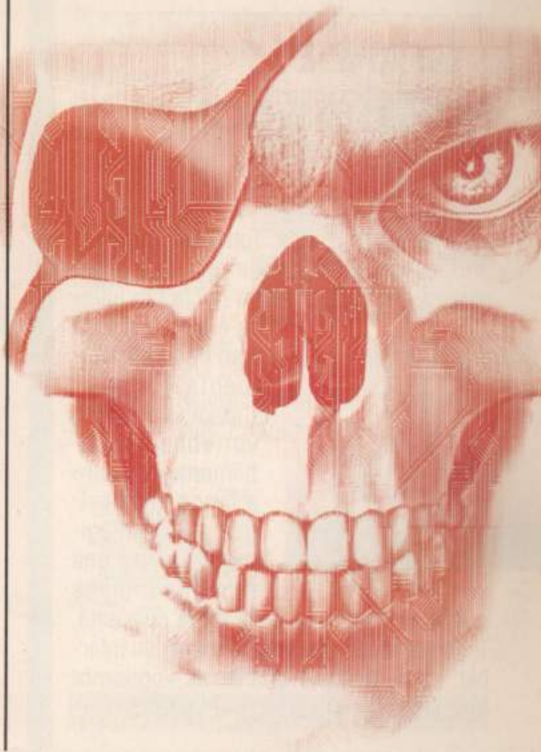
Gianluca

A parte il fatto che, forse, l'utilizzo di un antidialer freeware (tra i tanti, per esempio: http://www.digisoft.cc/download.htm#AntiDialer) avrebbe risolto la questione posta dal tecnico senza spese ulteriori, è indubbio che le prestazioni dell'ADSL sono comunque superiori. Quindi, per valutare i costi, è necessario capire, prima di tutto, quanto tempo si usa Internet e quanto il telefono. E guardare con quest'occhio tutte le offerte ADSL nella propria zona, valutando la più conveniente. Passare ad ADSL non è mai un errore, ma dipende molto da cosa si vuole fare.

INNO A TE, HACKER

Onore e gloria a Voi,
indomiti Guerrieri
A Voi che cavalcate tastiere
e non destrieri
A voi che giorno e notte,
combattete senza affanno
Il re della finestra,
mentore di ogni inganno
Moderni Robin Hood,
va darà ragion la Storia
Ovunque adesso siate,
a Voi onore e gloria.

HACKERS (by Taz)



HOT!

UTILIZZATORI DI ICQ SOTTO ATTACCO!

50 mila pc sono già stati infettati dal worm Bizex, che usa gli utenti ICQ invitandoli a linkarsi al sito jokeworld.biz, da cui parte l'attacco che sfrutta, manco a dirlo, le vulnerabilità di Internet Explorer e Windows. Dopodiché il worm manda lo stesso invito a tutti quelli che abbiamo in lista tra i contatti ICQ. Inoltre racoglie qualunque informazione trovi sulla macchina infettata e che riguardi numeri di carte di credito o gli account relativi ai sistemi di pagamento di Wells Fargo, American Express UK, Lloyds, Barclaycard, Credit Lyonnais, e E*TRADE. Per finire, il nostro worm intercetta e raccoglie tutti i dati delle comunicazioni https (la versione criptata di http) e li invia a un server remoto. Insomma, un malizioso 'succhia quattrini' da cui difendersi con la solita precauzione: teniamo aggiornato il sistema, installiamo tutte le patch di Windows e adottiamo sempre un buon antivirus aggiornato costantemente da remoto.

GRANDE FRATELLO EPSON

http://www.theepsonfamily.co.uk/ è il link dove possiamo vedere per sei mesi la vita di una famiglia inglese in tutti i suoi particolari. Tutti? No, non proprio, ovviamente. Anche perché a differenza del Grande Fratello qui la famigliola è unita da un tran tran assolutamente normale. L'inziativa di Epson vorrebbe, probabilmente, studiare a fondo quali esigenze di 'immagine' può avere una famiglia inglese media. Per noi una delle tante curiosità. Tutto sommato di coppie piccanti, su Internet, se ne trovano quante ne vogliamo. Invece questa sì, che è una notizia!



TOSHIBA TI FULMINA!

Abbiamo un TV portatile Toshiba 15V11D 15"? Bene, facciamolo subito sostituire! Perché tutto il nostro impianto televisivo, compresi i lettori DVD, VHS o quanto altro attaccato al televisore, sono sotto tensione e basta toccarli per prendere la scossa. Finora non sono stati segnalati infortuni, ma perché dovremmo essere noi i primi?
I numeri di serie degli apparecchi potenzialmente difettosi sono quelli compresi tra 102-2416401 e 102-2417400 e la prima cosa da fare è telefonare subito al servizio clienti Toshiba 035.4242859 per mettersi d'accordo sulla sostituzione gratuita. E' inutile tornare dal rivenditore dove l'abbiamo acquistato: non potrà farci nulla.

TOSHIBA Italia

AVVISO DI RITIRO PRODOTTO

TV PORTATILE TOSHIBA 15V11D 15"

Si prega di notare che il potenziale difetto riguarda esclusivamente il modello di tv portatile Toshiba 15V11D

I numeri di serie degli apparecchi potenzialmente difettosi sono quelli compresi tra:
102-2416401 e 102-2417400

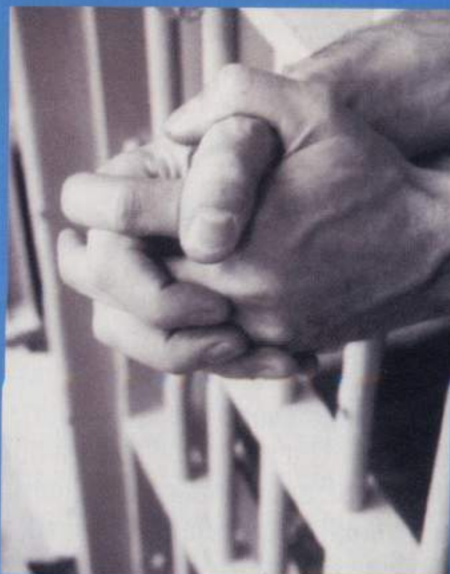
TOSHIBA Europe GmbH · Hammfelddamm 8 · D-41460 Neuss

DIAVOLO DI UN DEVOLO

Attacchiamo uno scatolino alla presa di corrente e siamo collegati a Internet in tutta la casa: tramite le prese della luce. Qualcuno ci aveva già provato, con risultati non sempre entusiasmanti. Questo sistema di Devolo, invece, pare promettere molto bene. Niente più cavi, solo un adattatore vicino al modem ADSL dove arriva la linea e un altro adattatore ovunque serva per avere, su un'uscita USB, Ethernet o wireless, la connessione a 14 Mbps massimi o 11 Mbps se wireless. E i disturbi sulla rete elettrica? Praticamente nulli in uscita, comunque inferiori a quelli di qualunque elettrodomestico. Mentre la resistenza alle interferenze, punto debole di tutti i sistemi di questo tipo, è abbastanza assicurata dalla codifica adottata. Esiste anche la versione 'audio', che ci consente di portare il segnale dell'impianto stereo in tutta la casa, senza fili. Tutte le info a www.devolo.it, e forse abbiamo risolto anche il nostro collegamento a Internet in cantina, dove nemmeno Wi-Fi è in grado di arrivare.

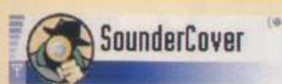


TV DIGITALE: IN AMERICA INIZIATI GLI ATTACCHI



Ha inviato via email un programmino spacciandolo come un miglioramento del software già installato. Così è riuscito a intrufolarsi negli scatolotti della TV digitale di diciotto americani abbonati a MSN-TV, reindirizzando tutte le telefonate dei servizi interattivi ai servizi di emergenza americani: il 911 equivalente al nostro 113. L'hanno anche beccato: si chiama David Jeansonne, ha 43 anni e adesso è incriminato come cyberterrorista. Ma ha anche dimostrato quanto la diffusione di sistemi meno sofisticati di un pc e ugualmente collegati in qualche modo alla rete, possano diventare potenzialmente una bomba a orologeria in casa di milioni di utenti. Chissà quante altre notizie di questo tipo ci aspettano anche qui in Europa...

PRONTO? PRONTO? NON TI SENTO!



Squilla il telefonino e la situazione si fa imbarazzante. Come facciamo a dire a Chiara che siamo sulla spiaggia in compagnia di Laura, quando ci crede in viaggio per cercare lavoro? Niente di più semplice che rispondere alla chiamata aggiungendo un bel sottofondo di rumore del treno che sferraglia. Oppure un continuo di clacson che sosterrà la grande bugia dell'ingorgo, tale per cui arriveremo a casa solo domattina, o anche un bel temporale che, accidenti, non ci permette di uscire, mentre siamo sdraiati a prendere il sole. SounderCover (www.simeda.com) serve esattamente a questo: lo scarichiamo sul nostro Nokia, associamo a ciascun nome della rubrica un bel rumore di sottofondo e siamo a posto.
Ogni volta che ci chiama quello scocciatore di Federico potremo sempre dirgli che siamo troppo impegnati a pilotare un aereo: alla riunione non arriveremo mai in tempo. Ma, ogni tanto, ricordiamoci di cambiare il rumore, perché alla lunga...

2000 FOTO PER SPIONI

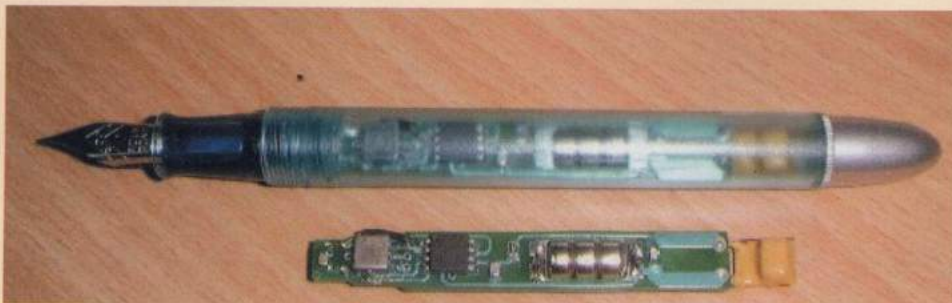
Clic, clic, clic, clic... così per duemila volte, mentre passeggiamo, andiamo a scuola, facciamo sport, facciamo l'amore... insomma sempre. È una ricerca Microsoft per una macchina fotografica digitale delle dimensioni di una tesserina stile carta di credito, attivata da un sensore di movimento. Tutto ciò che facciamo verrà registrato. Le persone che incontriamo verranno fotografate. Gli oggetti che vediamo saranno ricordati. E successivamente scaricati sul pc, inviati via Internet o tutto quello che potrà esserci utile per tenere traccia di quanto abbiamo fatto e visto durante il giorno.



Un comodo diario automatico o un bel sistema di violazione totale della privacy propria e altrui? Per ora è un prototipo presentato da Microsoft a Redmond, alla fiera TechFest. In seguito, vedremo.

PENNA DA AGENTI SEGRETI

Scrive e digitalizza: l'idea non è per nulla innovativa, ma la realizzazione è molto curiosa. La penna contiene tutta la circuiteria per tenere traccia dei movimenti e trasferire via radio al pc ciò che stiamo tracciando sulla carta. E' uscita sempre dai laboratori di ricerca Microsoft e, per ora, sembra un po' lenta nel funzionamento per avere qualche applicazione pratica immediata. Speriamo che, in caso di diffusione sul mercato, non sia da rifare troppo spesso il bootstrap, soprattutto se siamo abotuati a scrivere velocemente...



HOT!

PROPOSTO IL DOMINIO .XXX

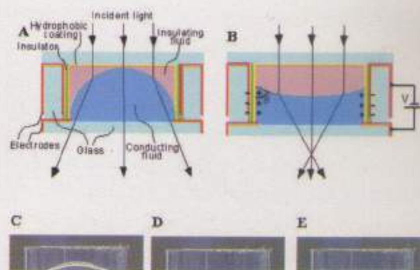
Detto così è uno scioglilingua, ma nove nuovi nomi sono quelli proposti ad ICANN da diversi consorzi, per aumentare i possibili domini Internet. Tra i nuovi nomi di dominio proposti ci sono: .xxx per i siti porno, .mobi per ciò che riguarda le comunicazioni mobili, .mail per la posta senza spam, .asia, .jobs, .tel, .post, .travel e .cat. Due mesi, a partire dal pimo aprile, saranno dedicati alla discussione pubblica di queste estensioni. Dopodiché la decisione di adottare questi nuovi TLD sarà presa verso fine anno. Se vogliamo spendere qualche minuto per dire la nostra: www.icann.org.



SPY-CAM CON L'OCCHIO FLUIDO

Servirà nei cellulari con macchina fotografica per mettere a fuoco istantaneamente i soggetti inquadrati, esattamente come fa il nostro occhio. E' prodotta da Philips (www.philips.com)
Si tratta di una lente che possiede la caratteristica di adattarsi a ciò che vede, senza dispositivi meccanici. Spessa tre millimetri, contiene un fluido che passa da una forma concava a una convessa tramite un campo elettrico. Riesce a mettere a fuoco dall'infinito a cinque centimetri. Perfetta, per le spy-cam!





Decreto Urbani:

Scambiarci file di materiale protetto da copyrigt ci mette subito nei guai. ***Giusta difesa della proprietà intellettuale*** *o azione da sceriffo del Web?*



▲ *Il ministro Urbani firma contento il decreto contestato.*

Ci confiscano tutto con il nome sui giornali

Riassumiamo: chiamato con il nome del ministro che l'ha proposto, il "ministro per i beni e le attività culturali" Giuliano Urbani, è stato approvato dal governo un decreto legge che sanziona lo scambio di opere cinematografiche protette da diritto d'autore.

Per i poveri mortali significa che non è più possibile scambiarsi via Internet, in qualunque modo, i file di film e dvd, o anche solo parte di essi, perché si rischia la confisca di tutto il materiale usato, computer compresi, la sanzione di 1.500 Euro e la gravosa e offensiva pubblicazione del nome in apposite liste su quotidiani e riviste specializzate del settore (del settore dello spettacolo!).

È legge italiana dal 12 marzo scorso. È ciò che in Rete viene definito dagli utenti "il famigerato Decreto Urbani", che possiamo leggere interamente a http://www.beniculturali.it/download/DL_Cinema_PCM12032004.pdf

Sessanta giorni, poi il buio

Non è finita. La promessa... urbana, è che entro sessanta giorni verrà esteso non solamente alle opere cinematografiche, ma con analoghe modalità anche allo scambio di file musicali, mp3, software, opere letterarie e qualunque altra opera dell'ingegno. Ingegnoso... Saremo quindi impossibilitati a usare qualunque programma p2p, pena le sanzioni e le denunce, la confisca e le liste di proscrizione pubblicate sui giornali.

Ma faranno sul serio? I dubbi ci sono, come si può vedere dal forum utenti di Puntoinformatico (www. puntoinformatico.it) dove qualcuno obietta che lo scambio tra privati di opere d'ingegno è comunque perseguibile con pene pecuniarie di ben inferiore portata (qualche centinao di Euro) e che, quindi, verrebbe a costare ben di più, allo Stato, imbastire tutto il processo che non lasciare perdere. Quindi l'ennesima bufala per terrorizzare gli utenti, istigata dalle grandi case di produzione cinematografica, che come vecchi e obsoleti dinosauri stanno dando gli ultimi colpi di coda? Il vero problema è che, in questo clima, è facile beccare un po' di utenti qua e là per dare certezza che si sta facendo sul serio, e indubbiamente il livello di rischio è passato da uno sbiadito giallino al rosso vivo.

Inviato: Mer Mar 17, 2004 4:08 pm   Soggetto:
Ben detto Gordon, è così che si parla!!
Secondo me questa legge è ingiusta!
Non fanno altro che indurre la gente a comprare i cd dai marocchini!
Prima potevamo tranquillamente scaricare o scambiare materiale!
Non è giustooooo!!!!!

sacrosanto o ECCESSIVO?



CI BECCANO CON LA PAURA

Abbiamo sempre sentito che i sistemi p2p sono fichi perché non scarichi da nessun server ma direttamente da un altro utente, ma allora come faranno a beccarci? I provider che non comunicheranno chi utilizza i sistemi p2p sono sanzionati con multe che vanno dalla bellezza di 50 mila a 250 mila Euro. Un bel mezzo miliardo delle vecchie lire se non diranno chi si è collegato, come e quando.

La protesta s'accende

Naturalmente la comunità degli internauti non può che reagire. Una petizione è già in linea al link http://no-urbani.plugs.it/. A dire il vero non ci sembra un'idea molto furba: la contestazione di una legge è assolutamente legittima, ma leggendo il testo sembra più una forma di autodenuncia. Altre forme di protesta stanno già circolando o sono promesse, nel tentativo di scardinare gli enormi interessi che circolano intorno al problema. Ne è un esempio chi ha già deciso di rinunciare all'ADSL (inviando disdetta almeno due mesi prima allo scadere del primo anno) per innescare un giro che di virtuoso ha tutto e il contrario di tutto: costringere i grandi provider delle telecomunicazioni, che così perderanno soldi in quantità, a premere perché i colossi dell'industria musicale e cinematografica facciano un passo indietro. Battaglie tra giganti istigate dal popolo? Staremo a vedere… Ma altri circostanziano bene e documentano quanto di perverso ci sia nel recente decreto: tra questi, per esempio, l'associazione ALCEI, http://www.alcei.it /documenti/copyright/p2panalisi.htm, piuttosto che l'associazione italiana degli internet provider (http://www.aiip.it/).
Queste ci sembrano battaglie da sostenere a spada tratta, perché in questo caso solo il numero farà la forza.

P2P non vuol dire pirateria

Chi può ancora pensare che Internet, la libertà d'informazione per eccellenza, per di più in un mondo in cui tutti gli uomini ragionevoli invocano libero scambio tra culture e sempre maggiore reciproca conoscenza, possa essere imbrigliata da leggiucole dettate dalla poca fantasia di interessi che sembravano immutabili? Ecco, il punto: difendiamo certamente i diritti d'autore, ma con uno sforzo di fantasia e creatività che coinvolga e invogli al rispetto reciproco, perché gli interessi siano interessi di tutti. Purtroppo la vittoria è ancora lontana: anche la RIAA, l'associazione delle case discografiche americane, sta stringendo il cerchio. Ha attivato altre cinquecento denunce a danno di universitari e ragazzini (http://www.riaa.com/news/newsletter/032304.asp) che sborseranno in media tremila Euro a testa di multa.
Tempi duri. ■

Chiuderemo il FORUM?

Sapete perché non leggerete più articoli sul p2p e programmi vari né su HJ, né sul forum on-line? Ecco, ancora il decreto:
"Chiunque pone in essere iniziative dirette a promuovere o ad incentivare la diffusione delle condotte di cui al comma 3 (l'articolo scandaloso, n.d.r.) è punito con la sanzione amministrativa pecuniaria di euro 2.000 e con le sanzioni accessorie previste al medesimo comma".

FASTSHARING FORUM

FASTSHARING CHIUDE.

Inviato: Mer Mar 17, 2004 10:39 pm   Soggetto:
straquoto gordon e fuocofatuo... sta legge l'ha scritta una persona che non ha la più pallida idea di come funzioni internet e i sistemi p2p...

mi sa tanto di demagogia...

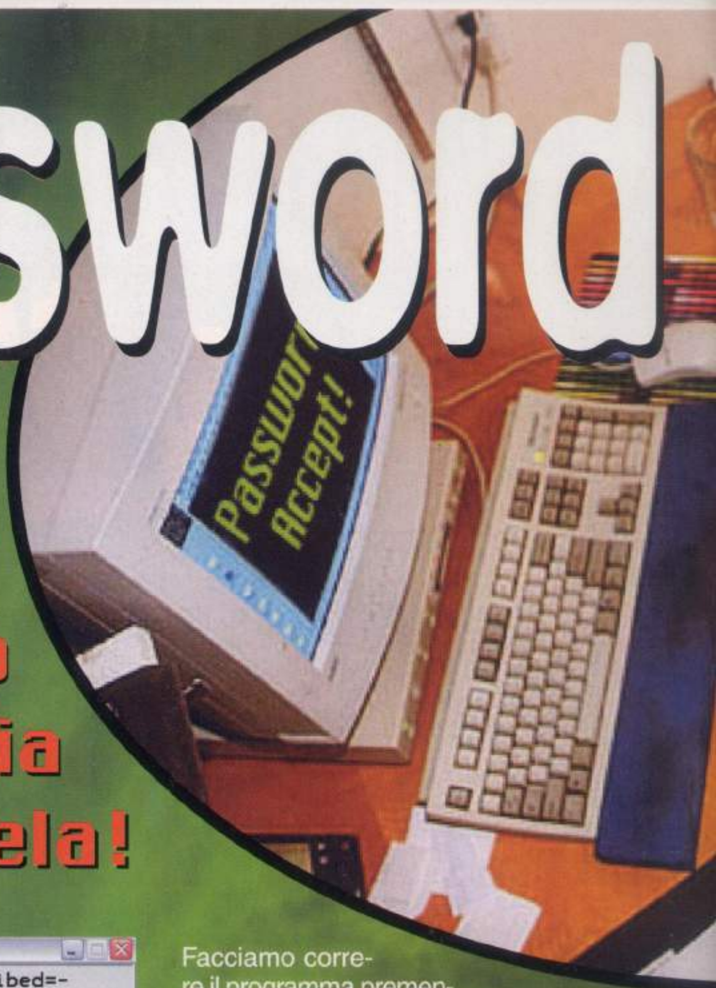
Inviato: Ven Mar 19, 2004 7:28 pm   Soggetto:
Si alla fine ci rimette sempre quello che non ha mai fatto niente di male... legge fa veramente schifo...è dura con i deboli e debole con i forti....nota manzoniana...

[il caos non è vuoto...
Ed il vuoto non è caos...]
Teoria del caos elaborata da me durante un'ora di matematica

Qualche forum è già stato chiuso e siti come Fastsharing (www.faastsharing.da.ru), vista l'aria che tira, hanno pensato bene di cessare la propria attività definitivamente.
Ma riusciranno davvero a imbavagliare il popolo della Rete?

La password

Il programma chiede una password? Modifichiamolo in modo che sia proprio lui a fornircela!

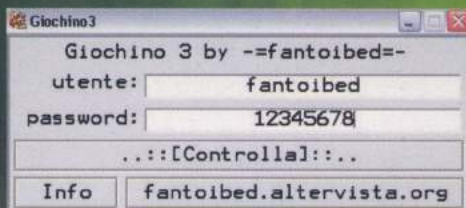


Che bello sarebbe poter leggere nel pensiero! La professoressa di latino ci interroga e, anche se il giorno precedente non abbiamo studiato nulla, rispondiamo correttamente a tutte le sue domande perché gliele leggiamo nella mente! Bello, no? Già, ma purtroppo è pura fantascienza, almeno nella vita reale. In ambito informatico, invece, un simile potere non è una remota chimera ma concreta possibilità per i reverser più smaliziati.

Peschiamo la password

La cavia dei nostri esperimenti è Giochino3, un piccolo programma scritto in linguaggio C che chiede un nome utente di almeno cinque caratteri e una password di 8 cifre esadecimali.

Apriamo il programma con OllyDbg e cerchiamo di determinare la parte di codice in cui viene confrontata la password corretta con quella che dobbiamo immettere noi. Scorrendo il listato di Giochino3 la parte che salta subito all'occhio è quella in cui compaiono in sequenza una chiamata alla funzione lstrcmpA (che serve a confrontare due stringhe), un salto condizionato (JNZ […]) e due chiamate alla funzione MessageBox: una per dirci che la password inserita è corretta, l'altra per dirci che è sbagliata. È ovvio che questa sia la zona del programma che stavamo cercando. Fissiamo un breakpoint subito la chiamata a lstrcmpA cliccando sulla riga 4016C8 e premendo F2.



▲ *Il programmino in C descritto nell'articolo, come appare in funzione.*

Facciamo correre il programma premendo F9 ed esso si aprirà sullo sfondo. Portiamolo in primo piano cliccando l'icona di Giochino3 nella barra di Windows e facciamo un tentativo con dei dati a caso, ad esempio "fantoibed" come utente e "12345678" come password. Premiamo il tasto "..::[Controlla]::.." e… zak! Siamo dentro la finestra di OllyDbg. Possiamo leggere chiaramente il contenuto del-

```
004016BD   68 60324000     PUSH main.00403260                          String1 = "12345678"
004016C2   FF15 0C204000   CALL DWORD PTR DS:[<&KERNEL32.lstrcmpA>]    lstrcmpA
004016C8   85C0            TEST EAX,EAX
004016CA  .75 1B           JNZ SHORT main.004016E7
004016CC   6A 00           PUSH 0                                      Style = MB_OK|MB_APPLMODAL
004016CE   68 5C314000     PUSH main.0040315C                          Title = "Bravo!"
004016D3   68 64314000     PUSH main.00403164                          Text = "Hai risolto il giochino 3"
004016D8   8B15 78324000   MOV EDX,DWORD PTR DS:[403278]
004016DE   52              PUSH EDX                                    hOwner => 0023030A ('Giochino3',class='fanto')
004016DF   FF15 28204000   CALL DWORD PTR DS:[<&USER32.MessageBoxA>]   MessageBoxA
004016E5  .EB 18           JMP SHORT main.004016FF
004016E7  >6A 00           PUSH 0                                      Style = MB_OK|MB_APPLMODAL
004016E9   68 80314000     PUSH main.00403180                          Title = "Spiacente!"
004016EE   68 8C314000     PUSH main.0040318C                          Text = "La password non è corretta!"
004016F3   A1 78324000     MOV EAX,DWORD PTR DS:[403278]
004016F8   50              PUSH EAX                                    hOwner => 0023030A ('Giochino3',class='fanto')
```

▲ *Il disassemblato del programmino*

PROFESSIONE DEBUGGER

OllyDbg, usato in questo articolo, è un debugger che lavora a livello di codice assembler e lo possiamo trovare sul Web all'indirizzo: http://home.t-online. de/home/Ollydbg/.



DIMMELA TU!



le due stringhe che sono appena state confrontate. Una è quella inserita da noi e l'altra è quella corretta! Volendo, potremmo scriverci su un pezzo di carta la password relativa al nostro nick e vivere felici e contenti ma, siccome siamo incontentabili, vogliamo andare oltre il semplice fishing e trasformare il giochino in un generatore di password in modo tale che, al posto della scritta "La password non è corretta", compaia direttamente la soluzione che stiamo cercando!

Modifichiamo il giochino

Chissà quali pesanti modifiche dovremmo apportare al programma per rendere possibile una tale magia! Hehehe, niente di preoccupante, basta modificare un paio di byte! Guardiamo la parte di programma successiva al punto in cui abbiamo fissato il breakpoint: c'è un salto condizionato che serve a mostrare l'una o l'altra delle due MessageBox a seconda che la password immessa sia corretta oppure no. Prestando un minimo di attenzione al listato visibile nella finestra del debugger, presente anche in queste pagine sotto forma di screenshot, notiamo che la soluzione esatta è memorizzata all'indirizzo 403250 e quindi possiamo modificare la riga 4016EE in modo che l'indirizzo passato alla MessageBox sia quello della password che ci serve. Per ottenere ciò apriamo l'eseguibile con hiew, premiamo due volte "invio" per impostare la visualizzazione in modalità "assembly", premiamo F5 e scriviamo ".4016EE" (attenzione al punto davanti). Entriamo in "edit mode" premendo F3 e modifichiamo la riga da "688C314000" che corrisponde a "push 0040318C" in "6850324000" che codifica l'istruzione "push 00403250"; rendiamo effettive le modifiche al file premendo F9 e usciamo con F10.

```
00000AE7: 6A00          push 000
00000AE9: 6880314000    push 000403180
00000AEE: 6850324000    push 000403250
00000AF3: A178324000    mov  eax,[0004032781]
00000AF8: 50            push eax
00000AF9: FF1528204000  call d,[0004020281]
```

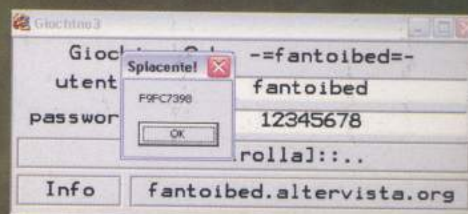
▲ *Bisogna andare a colpire qui!*

Giochino3
Spiacente!
La password non è corretta!
OK
by -=fantoibed=-
fantoibed
12345678
..::[Controlla]::..
Info
fantoibed.altervista.org

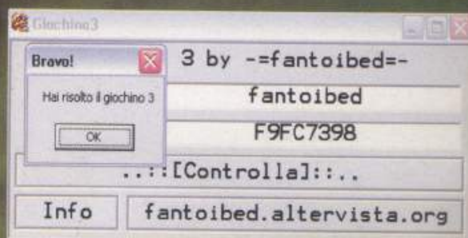
▲ *Prima della nostra modifica*

Conclusioni

A questo punto possiamo far partire la versione modificata del programma, che si comporterà come un generatore di password. Mettiamo il nostro nome ed una password a caso di 8 cifre esadecimali e cliccando sul tasto centrale, o premendo Invio su una delle due editbox, otterremo una messagebox che ci fornirà la soluzione corrispondente al nome inserito. Prima di chiudere vale la pena di ricordare che queste tecniche non devono essere usate per utilizzare a scrocco software commerciali, ma solo per l'interoperabilità o l'analisi dei programmi, come previsto dalla legge italiana sul diritto d'autore. Ciao!



▲ *Dopo la nostra modifica.*



▲ *Come si comporta il programmino se viene inserita la password corretta.*

nick fantoibed
fantoibed@libero.it

GIOCHINO3 IN SECRET ZONE

Il programma Giochino3 si trova nella Secret Zone del sito di Hacker Journal, http://www.hackerjournal.it

Cronaca di un ATTACCO al



Un giorno d'inverno piovoso, la solita e inutile lezione di informatica. Tutti in laboratorio, come bravi bambini. Ma d'un tratto ...

Una giornata come tante altre. Ci sediamo davanti al PC dell'aula informatica e d'un tratto lo guardiamo con un occhio diverso. È lì, parzialmente difeso da una scatola chiusa con un lucchetto. È come avere addosso, tutt'un tratto, una smania di ricerca, di sfida. Un non so che di presunzione di commettere un'azione deprecata da molti, ma nello stesso tempo dimostrare la propria capacità.
Lo guardiamo e, in fondo in fondo, non è poi così inaccessibile: c'è la possibilità di inserire CD e floppy. Poi lo conosciamo, l'abbiamo già usato: il solito, e bacato, Windows 2000 Professional, un bel antivirus Symantec non disattivabile e, lo sanno tutti, l'account Docente accessibile senza password - gruppo: users.

La sfida si è inserita in un angolino del nostro cervello. Non si può più tornare indietro, dobbiamo provarci, è una sensazione… di eccitazione imminente.
Inseriamo un floppy di boot e un CD di boot nel PC e accendiamo. Se funzionasse otterremmo una shell di DOS, ma sfortunatamente l'admin ha settato il BIOS in modo che segua la seguente precedenza:

1) Hard-disk
2) Cd-Rom
3) Floppy

Se l'admin si fosse dimenticato di settare la password al BIOS non avremmo problemi, ma cliccando CANC all'avvio abbiamo subito notato che era settata e quindi siamo leggermente più nei guai di quanto ci aspettavamo. Ma non ci arrendiamo certo per così poco!
Ci siamo loggati dentro e abbiamo preso un paio di informazioni. Dimentichiamo tutto quello che pensiamo di sapere su pwdump e samdump che dovrebbero estrarre la lista degli account per poi elaborarli con lophtcrack: non è vero! L'abbiamo scoperto a nostre spese, non funzionano e inoltre si deve essere amministratore per poterli usare, quindi l'unico modo per risolvere è installare sul computer lc4 e farli estrarre da lui. Peccato però che per poterle estrarre avremo bisogno di appartenere al gruppo administrator. Quindi a questo punto la domanda è: come facciamo a diventare administrator?

Diventare admin

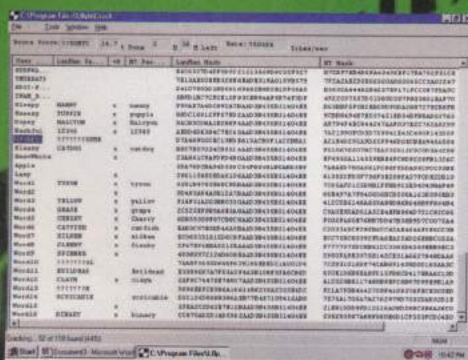
Inizialmente pensiamo di usare il programma sechole.exe, che ci permette di diventare administrator, ma non funziona su tutti i Windows e inoltre, accidenti, c'è l'antivirus attivato che non ci permette di farlo partire. Riavviamo Win2000 e clicchiamo F8. Lanciamo la modalità provvisoria e rinominiamo C:\programmi\symantec in C:\programmi\symantec1 in modo che all'avvio successivo non trovi più la cartella con l'antivirus. Un colpo ben assestato: niente antivirus, ma sechole non funziona.
La questione comincia a farsi gustosa.

SERVER della SCUOLA

L'unica soluzione è eliminare la pass del BIOS e su Internet ci sono tantissimi programmi che lo fanno con successo, come awcrack.exe, ma non funzionano su Windows2000, per un problema di sistema operativo non si può interagire con il BIOS... Campanella, lezione finita. Frustrazione momentanea di non essere ancora riusciti a combinare nulla. Ma il tarlo mentale lavora, e lavora...

A casa

È come un loop cerebrale, è lì che funziona, funziona anche se non ci fai caso, funziona anche se non ci pensi, non ci vuoi pensare, ma... eccome se ci pensi. E infatti, di botto, eccola lì, la soluzione!
Quando una scheda madre parte c'è una funzione che si chiama SKIP e che si può



richiamare per farle saltare il riconoscimento dell'hard disk e del CD-Rom. Quindi se quella stramaledetta scheda non avesse visto hard disk e CD-Rom l'avremmo fregata: avrebbe fatto partire il floppy!

Il mattino dopo

Eccoci di nuovo, sei qui, ora ti avrò in pugno. Facciamo lo skip e come volevasi dimostrare: parte il floppy! Abbiamo inserito un floppy di boot di Win95. Ottenuta la shell l'abbiamo estratto. Inseriamo un floppy della nostra valigetta per le emergenze di questo tipo... che contiene awcrack.exe e via, lanciato.
Da una shell di DOS funziona a meraviglia! Riavviamo, settiamo il BIOS perché possa vedere come primo boot il floppy. Riavviamo di nuovo, riparte la shell, mettiamo un altro dischetto con dentro:

```
awcrack.exe
ntcp.exe
sysshell.exe
```

Win2000 si basa su una partizione NTFS che naturalmente la FAT32 del floppy non legge, per cui usiamo ntcp.exe:

```
ntcp//hda1/winnt/system32/spoolsv.exe
//hda1/winnt/system32/spoolsv.old
ntcp sysshell.exe //hda1/winnt/
system32/spoolsv.exe
```

Riavviamo...

Aperta parentesi:
Systemshell (sysshell.exe) è un programma che sostituito a spoolsv.exe all'avvio fa apparire una shell con privilegi di administrator.
//hda1 <— Primo hard-disk prima partizione (come dire C:)

Voilà! Ci siamo loggati come docente ed ecco la nostra shell!

net localgroup administrators docente /add

Riavviamo...

Ho tolto sysshell.exe
Shell del dischetto e:
ntcp //hda1/winnt/system32/spoolsv.old //hda1/winnt/system32/spoolsv.exe

Riavviamo...

Siamo admin! Installiamo subito lophtcrack 4.0 e scarichiamo un dizionario di parole italiane e il crack per il programma che è a pagamento (st...zi!) Becchiamo le pass e salviamole per sicurezza su un floppy.

"E quindi il problema della sicurezza dei computer è sempre molto sentito, e i consulenti che il mondo aziendale cerca di assumere sono spesso ragazzi come voi che hanno approfondito le conoscenze e studiato a fondo le reti e il computer, come dovrete fare voi, se vorrete riuscire a combinare qualcosa nella vita!"
Mi entrava da un orecchio il solito blaterare del prof, che a volte era anche simpatico, ma vive in un mondo che sembra alieno... Ma intanto non mi guarda e posso cominciare a craccare le pass.

Lophtcrack 4.0 su un Athlon 1050mhz e 256ram ddr trova:

|lunghezza pass|	|tempo|
Minore di 7	Max 10 min.
Tra 7 e 13	Max: 6 ore
14	Max 12 ore

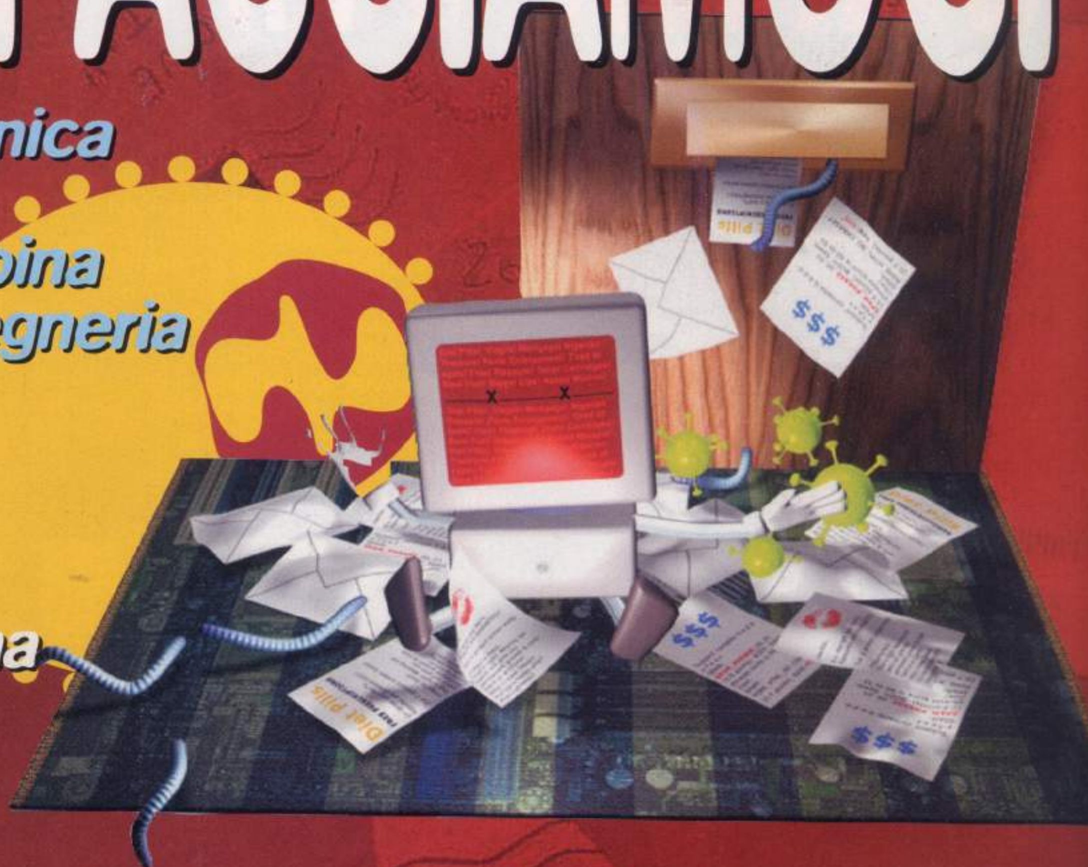
Fatto! Una mattinata ben spesa.

Witch_blade



NON FACCIAMOCI

Una nuova tecnica di spamming via email combina trucchi da ingegneria sociale con codice HTML, per fregarci informazioni (e soldi) appena possibile



L'INIZIO È UN CLASSICO, MA È STUDIATO BENE. RICEVIAMO UNA EMAIL DI QUESTO TENORE:

Buongiorno.
Ci risulta che la polizia stia investigando su di voi. E' vero? Avete realmente commesso qualche crimine? Non esitate a leggere l'articolo che trovate presso:
http://federalpolice.com:
article872@1075686747
o all'indirizzo
http://0100.035.0255.0133

Cordialmente,
un vecchio amico

Ovviamente questo messaggio ci mette addosso un po' di paura e siamo portati a provare i link suggeriti.

Diamo un'occhiata al primo:

http://federalpolice.com:article872@1075686747

La costruzione della prima parte di questo URL è un trucco molto usato: tutto ciò che sta prima della "at" è generalmente il metodo utilizzato per inviare uno UserID e relativa password via http. Ma se il server che la riceve non ha nessun sistema di riconoscimento di identificativo utente e password, l'unico pezzo dell'URL che rimane in piedi è il secondo, dopo la @.

Per cui noi crediamo, a prima vista, di contattare un sito di nome federalpolice.com, ma in realtà stiamo semplicemente contattando

http://1075686747

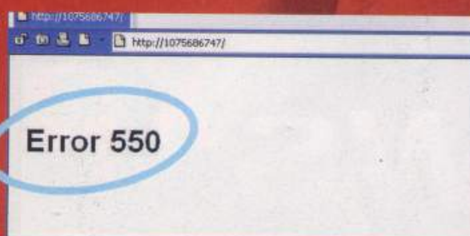
Anche se questo sembra un indirizzo senza senso, perché non appare nella forma classica degli indirizzi IP, in realtà è semplicemente un nome che decodificato porta al vero indirizzo IP, che nel caso reale in questione punta a:

http://64.29.173.91

Il secondo URL che l'email ci suggerisce sembra proprio un indirizzo IP, ma se lo guardiamo bene non lo è per niente. Gli spammer hanno utilizzato anche in questo caso un sistema di copertura dell'indirizzo IP chiamato "hex/octal overflow", che i browser decodificano al volo per puntare allo stesso indirizzo.

FREGARE!

Se decidiamo di andarlo a visitare, ci troviamo davanti a un classico messaggio d'errore:



che in genere significa che uno script dal lato server ha avuto dei problemi di funzionamento. All'apparenza niente di grave, e siamo così indotti a lasciare perdere. MA ORMAI IL DANNO È FATTO.

Quella che vediamo, infatti, è una normale pagina HTML che contiene il finto messaggio d'errore e che invece installa una applet Java che richiama un file di nome javautil.zip che, a sua volta, non è un file .zip, ma un .exe mascherato. Per cui ci troviamo di botto un programma in esecuzione. Il file mascherato è stato creato con FSG (http://www.xtreeme. prv.pl/), un programma di packing piuttosto popolare tra i cracker, per comprimere e criptare trojan, worm ed altri ammenicoli... Proviamo a decomprimere il file trovato, magari utilizzando una macchina Linux per non rischiare l'infezione: il risultato è un bel trojan keylogger che monitorizza le finestre di dialogo per recuperare info rispetto a delle parole-chiave, tra le quali:

commbank, Commonwealth, NetBank, Citibank , Bank of America - e-gold , e-bullion , e-Bullion - evocash, EVOCash, EVOcash, intgold, INTGold - paypal, PayPal - bankwest, Bank West, BankWest - National Internet Banking - cibc, CIBC - scotiabank, ScotiaBank - Bank of Montreal - Royal Bank - TD Waterhouse - Wells Fargo Bank One - SunTrust - Discover Card - Washington Mutual - Wachovia - Desjardins - Chase

e parecchie altre stringhe simili. Quando trova una corrispondenza, memorizza tutto quello che scriviamo sulla tastiera in un file chiamato kng.txt, il quale viene inviato all'indirizzo

pentasatan@mail.ru

tramite un sistema di email integrato e automatico. Questa combinazione di tecniche di ingegneria sociale, spoofing degli URL, pagine web costruite ad-hoc e caricamento automatico di trojan fanno parte del sofisticato "phishing scam", la categoria di sistemi utilizzati per rilevare quanti più dati possibile per frodare banche, istituti di credito e enti che trattano denaro. E tutti quanti stanno organizzandosi per combattere il fenomeno che, oltre ad essere ampiamente illegale, mette a rischio anche il nostro salvadanaio.

APPLET JAVA

L'applet Java utilizzato per caricare sul nostro computer il file eseguibile mascherato fa parte di un insieme di classi Java (blackbox.class) che sono omai riconosciute dalla maggior parte degli antivirus attuali. Altre informazioni rispetto a questo tipo di codice le possiamo recuperare a: http://www.viruslist.com/eng/viruslist.html?id=72440

SERVER WINDOWS BUCATO

Il server che è stato utilizzato per la diffusione del tutto è un server Windows, crackato con NetBus (http://home.t-online.de/home/TschiTschi/nbv17.htm). NetBus è un programma che funziona così bene da essere anche legittimamente utilizzato da alcuni amministratori di sistema per il controllo remoto del proprio server.







Configurare più impostazioni di rete e creare file autoscompattanti si può fare in pochi clic, ecco i trucchi nascosti in Windows Xp



RETI E PORTATILI

Quando portiamo in giro il portatile, capita spesso di attaccarci a reti differenti, con parametri differenti. Ogni volta è un problema: dobbiamo aprire la connessione di rete, poi andare su Proprietà e lì decidere quali parametri inserire, in base alla configurazione della rete a cui ci stiamo collegando. Una bella seccatura. Che alcuni programmi risolvono, ma sono programmi shareware, che impiegano comunque diverso tempo a caricarsi e sistemare le cose e che vanno ad affollare la già ricca raccolta di applicazioni che ognuno di noi ha sul proprio hard disk.

Quando invece un comando di Windows semplifica enormemente le cose e, se non serve altro, è perfetto ai nostri scopi.

Andiamo su Start -> Esegui e battiamo cmd. Siamo dentro la finestra comando. Al prompt C:\> scriviamo

```
netsh -c interface dump >rete1.txt
```

dove al posto di rete1.txt possiamo scrivere il nome della configurazione attuale, per ricordarci quando dovremo usare gli stessi settaggi. Per esempio, se siamo a casa, potremmo scrivere 'Casa.txt', e così via.

Così facendo viene creato un file di testo (nella directory in cui si lancia il comando, nel nostro esempio C:\), contenente i parametri di configurazione per la rete attuale.

Facciamo lo stesso quando andiamo a scuola, in azienda, da un amico o in altri posti, creando diversi file di testo.

Quando ci servirà richiamare una configurazione, sarà sufficiente scrivere, sempre nella riga comando:

```
netsh -f rete1.txt
```

dove al posto di rete1.txt dobbiamo scrivere il nome del file corrispondente al posto dove siamo collegati.

C:\WINDOWS\System32\cmd.exe

```
C:\>netsh -c interface dump >rete1.txt

C:\>netsh ?

Sintassi: netsh [-a FileAlias] [-c Contesto] [-r ComputerRemoto]
             [Commando | -f FileDescrizioneProcedure]

Sono disponibili i seguenti comandi :

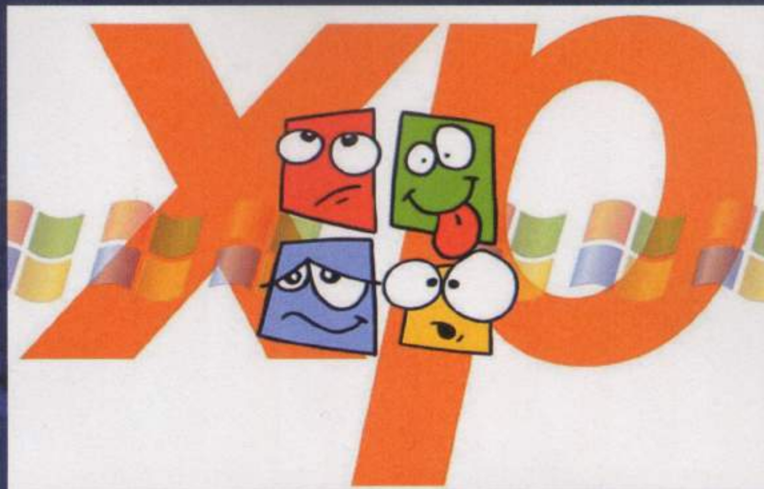
Comandi in questo contesto:
?              - Visualizza un elenco di comandi.
add            - Aggiunge una voce di configurazione a un elenco di voci.
bridge         - Passa al contesto `netsh bridge'.
delete         - Elimina una voce di configurazione da un elenco di voci.
diag           - Passa al contesto `netsh diag'.
dump           - Visualizza uno script di configurazione.
exec           - Esegue un file di script.
help           - Visualizza un elenco di comandi.
interface      - Passa al contesto `netsh interface'.
ras            - Passa al contesto `netsh ras'.
routing        - Passa al contesto `netsh routing'.
set            - Visualizza impostazioni di configurazione.
show           - Visualizza informazioni.

Sono disponibili i seguenti sottocontesti:
 bridge diag interface ras routing

Per vedere la guida per un comando, digitare il comando seguito da uno
 spazio e quindi digitare ?.

C:\>netsh -f
```

IExpress permette di creare file autoscompattanti in pochi clic e senza nessun software aggiuntivo



PIÙ VELOCE!

Durante la fase di compattazione dei file appare una finestra DOS in cui viene eseguito il programma Cabinet Maker. Se abbiamo inserito file piuttosto grandi o già compressi, il processo risulta piuttosto lungo. Massimizzare la finestra (con un clic sul quadrato a pieno schermo in alto a destra) lo velocizza notevolmente.



IMPACCHETTIAMO I FILE

Questo trucco ci è stato segnalato dal lettore RegMaster e riguarda un tool Windows nascosto e poco conosciuto, che permette di impacchettare diversi file in un unico .exe autoscompattante, creando un vero e proprio sistema di distribuzione di file, con tanto di possibilità di inserimento dei termini di licenza e guadagno di spazio per compressione. Usa uno wizard che ci accompagna in tutte le fasi di creazione del pacchetto, e si richiama da Esegui (Start) scrivendo:

```
iexpress
```

Appare una finestra in cui indicare se vogliamo creare un file autoscompattante o se vogliamo scompattarne uno.



Poi dobbiamo specificare se il file che stiamo costruendo dovrà autoscompattarsi e avviare un'installazione, oppure se dovrà solo decomprimersi nei file che lo costituiscono o ancora se sarà solo un file compresso, senza opzioni di autoscompattamento.

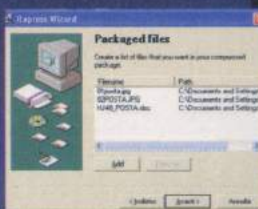


Alla terza schermata dobbiamo dare un nome al pacchetto, mentre alla quarta possiamo inserire un messaggio che apparirà all'utilizzatore finale e chiederà conferma prima di autoscompattare il file.

Ora possiamo anche inserire il richiamo a un file di testo contenente una licenza d'uso, o un testo di aiuto o quant'altro. Infine, con il pulsante Add, aggiungiamo i file che vogliamo impacchettare.



Se avevamo scelto di avviare un programma di installazione, a questo punto ci viene richiesto di specificarne il nome e possiamo scrivere anche un eventuale comando da eseguire alla fine dell'installazione stessa. Se invece avevamo scelto una semplice autoestrazione, dobbiamo specificare adesso in quale finestra di dialogo dovranno apparire i prompt con l'utente. Lasciamo Default, che è la scelta migliore.



Specifichiamo un eventuale messaggio di uscita e infine diamo un percorso e un nome al file risultante. Possiamo salvare tutti i parametri impostati per una prossima volta, poi finalmente creare il pacchetto: appare una finestra con qualche statistica.





Se il file non è molto grande, ciò che guadagnamo in compressione lo perdiamo in istruzioni per lo scompattamento. Un altro inconveniente è che, a differenza di un file .zip, inviando un .exe verrà immediatamente bloccato da tutte le protezioni antivirus.

Le MERAVIGLIE

Facciamo da soli qualche magico script per la gestione delle immagini all'interno di una pagina web

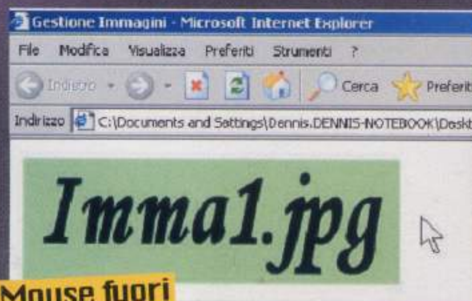


Con i Javascript si possono fare meraviglie, lo sapevate? Ecco alcuni tra i più interessanti e utili per migliorare le nostre pagine.

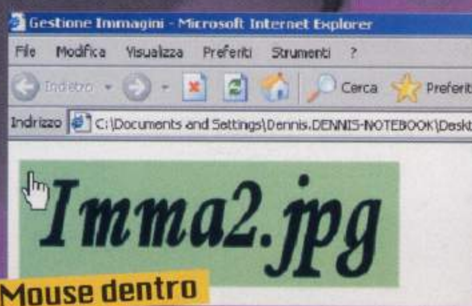
I rollover

I rollover sono gli effetti che possiamo creare quando con il mouse passiamo sopra un'immagine (evento onMouseOver) e quando usciamo dall'immagine (onMouseOut). Si usano spesso quando un'immagine rappresenta, in realtà, un link. Ecco un esempio:

```
<img src="imma1.jpg" style="cursor:pointer" onMouseOver="this.src='imma2.jpg'" onMouseOut="this.src='imma1.jpg'" />
```



Mouse fuori



Mouse dentro

Al passaggio del mouse l'immagine "prima.jpg" viene sostituita da "seconda.jpg".
All'uscita del mouse, ritorna tutto come prima. Viene inoltre settato un css (style="..."), in modo che il cursore cambi e diventi una manina.
Con la stessa tecnica possiamo agire anche su tasti di tipo image(<input type="image">).

Un altro tipo di rollover può essere quello che modifica le dimensioni di un'immagine:

```
<img src="imma1.jpg" style="height:100px;width:100px;cursor:pointer" onMouseOver="this.style.height='120px';this.style.width='120px'" onMouseOut="this.style.height='100px';this.style.width='100px'" />
```

di JavaScript

Effettuare il submit del form tramite un immagine

Per effettuare il submit (l'invio) di un form possiamo utilizzare sia un tasto di tipo immagine, sia un'immagine vera e propria.
Basta sostituire:

```
<input type="submit">
```

Con:

```
<input type="image" src="imma1.jpg">
```

Non è una vera e propria immagine, ma un input di tipo 'image', appunto. Nel caso volessimo effettuare il submit di un form attraverso una vera e propria immagine, agiamo sull'evento onClick dell'immagine stessa:

```
<img src="imma1.jpg" onClick="document.NOMEFORM.submit()" style="cursor:pointer;" />
```

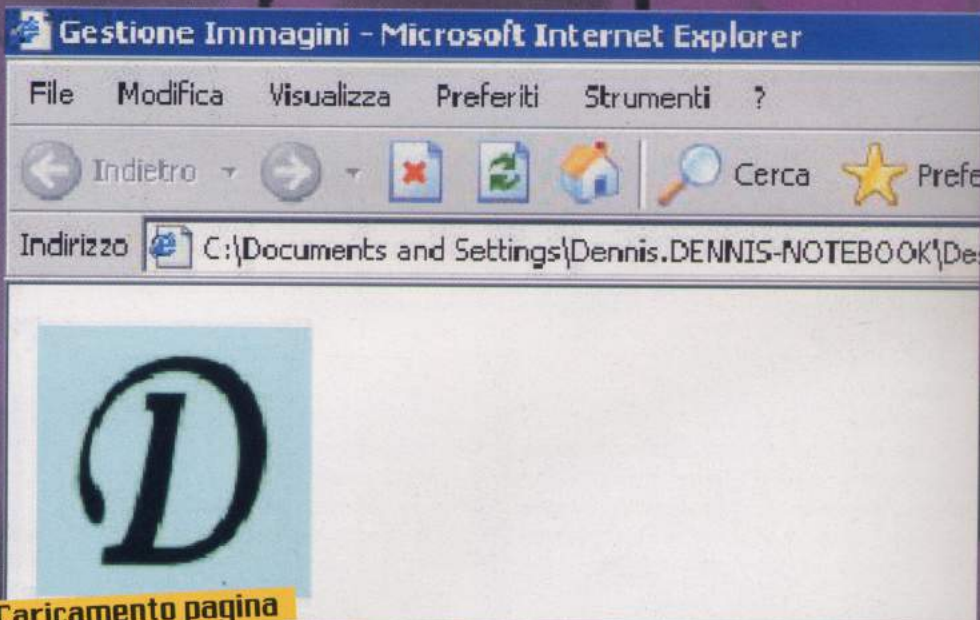
ovviamente NOMEFORM dobbiamo sostituirlo con la proprietà name del form da inviare.

Sostituire un'immagine presente con un'altra

Se dobbiamo sostituire un'immagine con un'altra, la strada da seguire è quella di creare una funzione che ci ridefinisca la proprietà src di una data immagine:

```
<script>
function cambia_immagine
(quale,nuova){
document.images[quale].src=nuova
}
</script>

<img name="immagine1" src="imma1.jpg" />
<input type="button" onClick="cambia_immagine('immagine1','imma2.jpg')" value="cambia immagine">
```



Caricamento pagina

In questo esempio abbiamo creato una funzione, richiamata al Click sul tasto. Se ci necessita di cambiare una sola immagine, si può tranquillamente agire come visto per i rollover, ovvero agire direttamente all'interno del tag input:

```
<input type="button" onClick="document.images['immagine1'].src='seconda.jpg'" value="cambia immagine">
```



Movimento mouse

Immagine che segue il mouse

Si chiamano mouse trailers, sono immagini (o livelli), che seguono il mouse su tutta l'area della pagina.

Su internet ne esistono moltissimi, se facciamo una ricerca su un motore di ricerca qualunque oppure in una raccolta di script ne troviamo a bizzeffe.
Per crearne uno semplice basta poco:

```
<script>
function segui(){
document.trailer.style.position="absolute"
document.trailer.style.top=event.clientY+15
document.trailer.style.left=event.clientX+15
}
</script>

<body onMouseMove="segui()">
<img name="trailer" src="imma1.jpg" style="width:100px;height:100px" />
```

poiché si agisce sulle proprietà top e left, il posizionamento dell'immagine viene settato dallo script ad "absolute", come necessario.
Nella funzione, vengono settati top (distanza dal bordo alto della pagina) e left (distanza dal bordo sinistro della pagina) con le posizione del mouse, aggiungendo 15 pixel ad entrambe, cosicché l'immagine resta un minimo distaccata dal puntatore vero e proprio

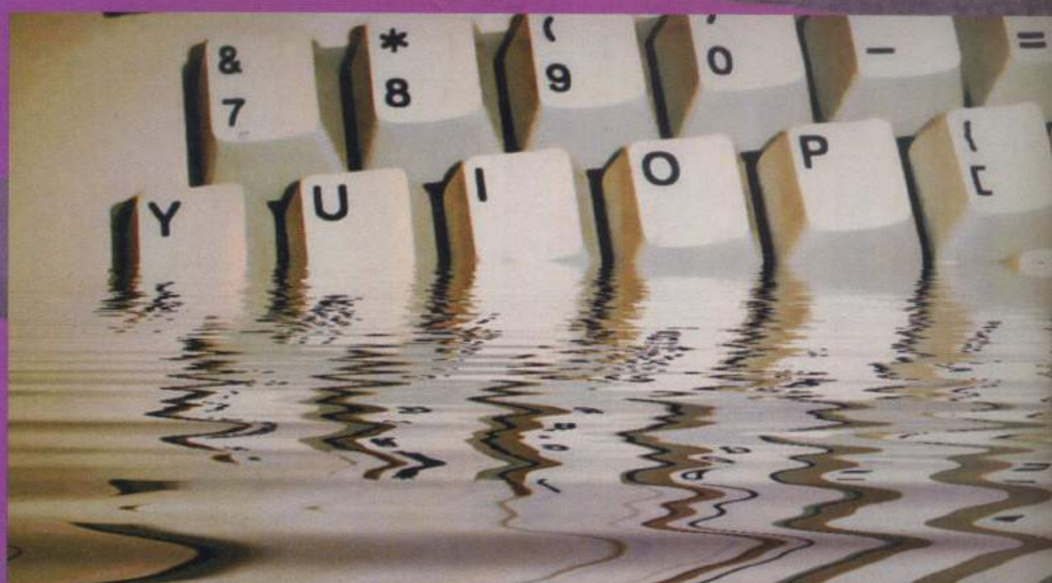


Immagine che segue lo scorrimento della pagina

È possibile utilizzare uno script di questo tipo per far scorrere un immagine (ma all'occorrenza un qualsiasi elemento), seguendo lo scorrimento del browser.

Ciò che si deve fare nello script è semplicemente settare le due variabili margineX e margineY, i margini che l'immagine manterrà rispettivamente dal bordo sinistro e dal bordo superiore della pagina.

```
<script>
function scorri(nome){
margineX=15;
margineY=30;
asseY=0;
asseX=0;
if(document.documentElement &&
document.documentElement.scrollTop){
	asseY=document.documentElement.scrollTop;
	asseX=document.documentElement.scrollLeft;
}
else if(document.body){

asseY=document.body.scrollTop

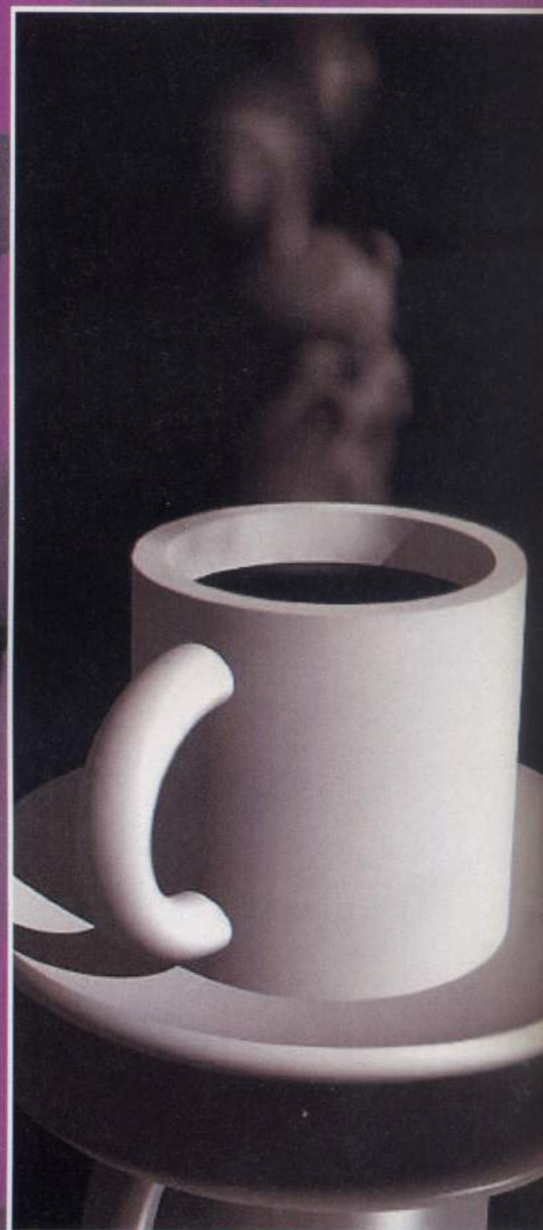
asseX=document.body.scrollLeft
}
document.images[nome].style.position="absolute";
document.images[nome].style.left=asseX+margineX;
document.images[nome].style.top=asseY+margineY;
}
</script>
```

questo script va richiamato semplicemente all'evento onScroll del body:

```
<body onScroll="scorri('NAMEIMMAGINE')">
```

Il codice risulta essere forse un po' più elaborato dei precedenti esempi, ma il funzionamento è semplice.
Poiché la funzione viene richiamata allo scroll (ovvero quando scorro la pagina), ridefiniamo ogni volta la posizione dell'immagine, e prendiamo i valori dello scroll raggiunto aggiungendo i margini fissati nello script. Purtroppo l'effetto funziona solamente su Internet Explorer e Mozilla (superiore a 1.0).
Con script opportunin possiamo anche immagini temporalizzate, immagini random, preload di immagini e altre operazioni con e sulle immagini. Scriveteci se ne volete sapere di più.

Pederiva 'Dennis' Danilo
pederiva_d@hotmail.com



ODORI VIA WEB

L'odore dell'amore, un profumo di fiori misto a pelle che sa di sole. Un modo nuovo per dirti ti amo... o la peggiore delle invenzioni possibili?!

Scarichiamo musica, filmati, videoclip, mp3, programmi, foto e chissà cos'altro. Ma abbiamo mai pensato agli odori? Eppure è proprio quello che fa il sistema sperimentato da Telewest Broadband, una delle più grandi società inglesi di fornitura di connettività. È un po' come se qui da noi Wind o Tiscali annunciassero una scatoletta che, collegata via USB al nostro PC, invece di farci stampare le foto ricevute via internet dalla ragazza lontana, ci fa sentire il profumo della sua pelle. Niente male, vero? Immaginiamoci la chat per trovare l'anima gemella. Che carattere hai? Cosa ti piace? E a parole è facile dirci che siamo fatti l'uno per l'altra, che il prossimo incontro non virtuale sarà quanto di più eccitante esista al mondo, ma... e se poi puzza? Invece così eccoci in diretta l'odore dei nostri sogni, il profumo dei nostri desideri. Anche quelli più perversi, se ci aggrada. Un bel puzzo della cosa più schifosa che ci viene in mente, da spedire all'amico, si fa per dire, che c'ha fregato la ragazza.

Il sistema funziona con collegamenti a larga banda e non chiediamoci perché, ma è nelle specifiche, miscelando opportunamente delle infinitesime gocce di liquidi appositi e poi sfruttando uno speciale spruzzatore: lo spray risultante potrebbe avere, sulla nostra immaginazione, effetti davvero da non credere. E non parliamo certo del profumo di torta di mele di nonna papera, che comunque potrebbe essere un buon augurio per il prossimo compleanno di nostra madre...

Anti stress

E diamo un calcio perfino allo stress: abbiamo di che piazzarci davanti al PC e programmare il tutto usando l'applicazione fornita insieme al sistema. Che giornata è stata? Diamo un punteggio al nostro stress, da 0 a 10. Con 6, il profumo di melagrano unito a una spruzzatina di violetta sarà l'antidoto giusto per rilassarci alla grande. Se scattiamo a 10, un più deciso tabacco miscelato ad altre dodici essenze simulate ci darà una calmata che nemmeno immaginiamo.

E che dire di quando ci sdraiamo in poltrona, una bel disco Jazz e l'odore di sigari e tabacco che si diffonde nella stanza, come nei più fetidi music-pub che abbiamo frequentato a New Orleans?

Realismo puro, in una scatoletta rossa con venti essenze per un totale di sessanta desideri diversi. Ma appena dopo la versione Lite che sarà commercializzata, avremo l'upgrade a duemila odori differenti, che potremo attivare al di là del mondo. I costi? 250 Euro per hardware e software, 25 Euro al mese per il collegamento a larga banda. È la trovata dell'anno, se non si risolve nell'ennesima bufala, come otto anni fa, quando apparve su internet un aggiornamento di tag HTML tramite i quali ci fecero credere (?) che era possibile inviare odori via Web.



▲ *Ecco la genialata: interfaccia USB, collegamento a larga banda. Costo delle cartucce? Non è dato di sapere, ma siamo già abituati a quello delle stampanti... Ulteriori informazioni? http://www.telewest.co.uk*

One4Bus
one4bus@hackerjournal.it

OGGETTO DEL DESIDERIO

Un GSM che preoccupa parlamentari e polizia. Costa un botto, MA SOGNARE non è ancora reato!



Un parlamentare olandese ha recentemente chiesto che venga dichiarato fuorilegge Cryptophone (http://www.cryptophone.de). Cryptophone è un cellulare GSM come tanti di fascia alta, che unisce le funzioni di telefono a quelle di organizer, ma al contrario di tutti gli altri cifra le chiamate. La cifratura avviene solo quando si parlano tra loro due Cryptophone, ma questo basta a mettere in apprensione le autorità. Infatti l'Olanda è il Paese europeo che pratica più intercettazioni telefoniche di chiunque altro e l'idea che esistano telefoni che non è possibile intercettare può non piacere. D'altro canto l'Olanda possiede anche leggi estremamente liberali sulla crittografia e quindi non dovrebbero esserci restrizioni all'uso di Cryptophone.

Intercettare una chiamata

Come ben sa la polizia, è difficile predire il cammino preciso che una chiamata prende all'interno della rete, ma non è così difficile intercettare una conversazione. Le chiamate cellulari viaggiano su fasci unidirezionali di microonde che si captano piuttosto facilmente, con l'aiuto di apparecchi come l'IMSI-Catcher.

Se si osserva con attenzione l'antenna di un ripetitore di segnali cellulari come quelle che si vedono un po' in tutte le città, si possono notare talvolta piccole parabole poste nella metà inferiore dell'antenna. Da quelle parabole partono i fasci di microonde di cui sopra. Non è difficile, per chi sa come fare, intercettarli, registrare tutto e separare l'una dall'altra le chiamate in corso con l'aiuto di un demultiplexer. Infatti le chiamate GSM sono sì certamente cifrate, ma dal telefono al ricevitore della cella in cui ci si trova. Da lì in poi non c'è più nessuna garanzia. Oltretutto la cifratura GSM è deboluccia e non ci si dovrebbe fare eccessivo affidamento.



▲ *Il formato è un po' ingombrante, ma con l'IMSI-Catcher l'intercettazione è assicurata*

I creatori di Cryptophone hanno lavorato piuttosto bene, creando il prodotto più open possibile. Hanno preso il codice di PocketPC, che paradossalmente pur venendo da Microsoft è più aperto e accessibile del più venduto Symbian, lo hanno rivoltato come un calzino toglien-

do tutti i buchi possibili (il software made in Microsoft, se fosse un formaggio sarebbe Emmenthaler) e ci hanno inserito gli algoritmi di cifratura, conservando le funzioni di organizer. Così Cryptophone funziona da cellulare, da agenda e anche da dispositivo per la cifratura delle chiamate. Al momento il codice sorgente è disponibile unicamente per Windows. Lo si può scaricare dal sito di Cryptophone, leggerselo, provare a compilarlo e magari migliorarlo, se si è capaci. per il 2004 i produttori contano di offrire il Cryptophone su altri sistemi operativi diversi , come Embedded Linux, Symbian e PalmOS, e anche di arrivare sulle piattaforme 3G (UMTS) e TCP/IP. Essendo open source, niente vieta di adeguare il sorgente anche a Linux o Mac OS X. Staremo a vedere.

La prova della voce

Oltre alla cifratura, naturalmente, le chiamate effettuate con un Cryptophone sono soggette a compressione della voce, come accade per ogni telefonata GSM. Il Cryptophone usa il codec CELP con frequenza di otto kHz. Il flusso di output garantito dal codec è di 4,8 kbit per secondo, adatto a viaggiare sulla tipica chiamata GSM da 9.600 bit per secondo. Il risultato finale è paragonabile a quello che si ascolta in una telefonata intercontinentale, con possibilità per il segnale di peggiorare nel caso ci si trovi in zone scarsamente coperte o disturbate. Per via della cifratura, là dove una normale chiamata con il GSM si degrada per via di un cattivo segnale, con il Cryptophone la qualità non peggiora, ma aumenta il ritardo nella conversazione tra quando uno parla e quando l'altro ascolta.



▲ *Una vera e propria valigetta da agente segreto per il proprio Cryptophone a prova di intercettazione*

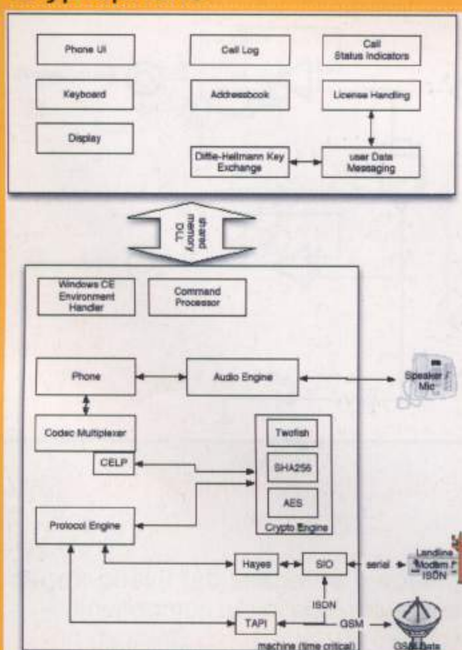
Caruccio questo telefono!

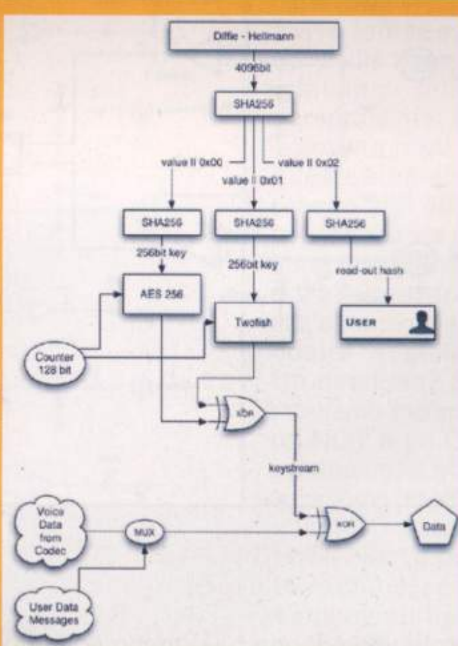
Eh, sì. Costa 1.799 euro. Comprandone due insieme si spendono "solo" 3.499 euro. La domanda da farsi è: quanto vale la propria privacy?

E i terroristi? E se viene usato per commettere crimini? È vero che Cryptophone permette di non farsi spiare le chiamate, ma prima di tutto bisogna averlo. E suppongo che, messi alle strette, i produttori del telefono tireranno fuori la lista degli acquirenti. Sono pochi a potersi permettere 1.800 euro di cellulare. Secondo, e ben peggiore per un criminale, la chiamata Cryptophone non può essere ascoltata, ma è una comune chiamata cellulare. I terroristi si sono già accorti a loro spese della pericolosità di un cellulare acceso. Al tempo della guerra in Iraq i giornalisti che non segnalavano alle truppe americane il proprio telefono satellitare rischiavano di vedersi arrivare un missile addosso nel giro di pochi minuti. Accendere un cellulare è come fare brillare il proprio puntino sulla mappa dei sospetti della polizia.

Michele Campovecchio
michele_c@hackerjournal.it

L'architettura del sistema Cryptophone



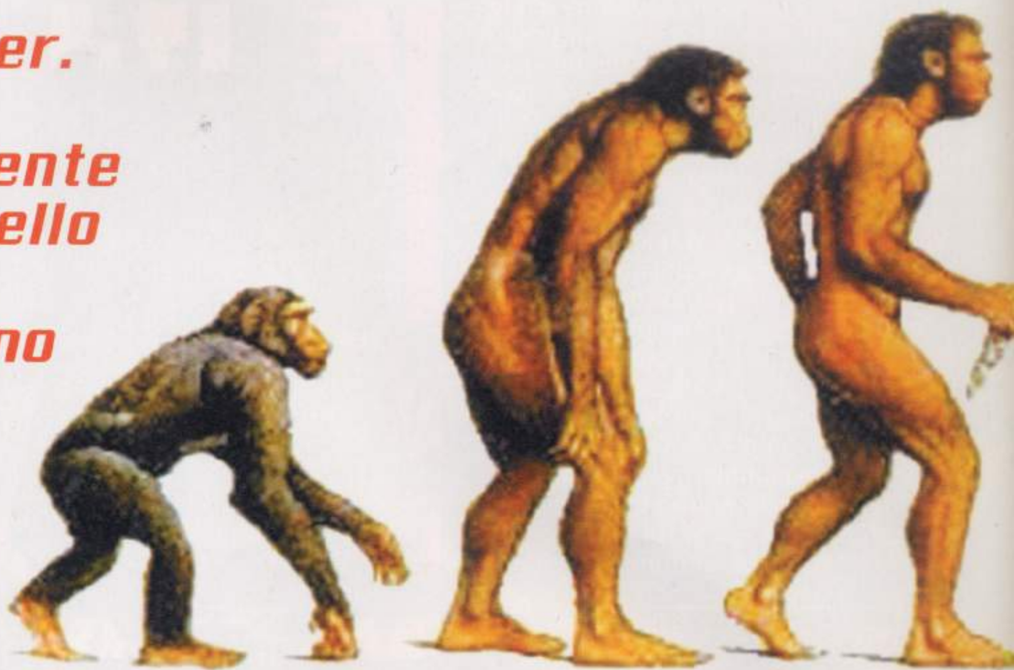


Come funziona la cifratura di Cryptophone

IMSI-CATCHER TI ASCOLTA

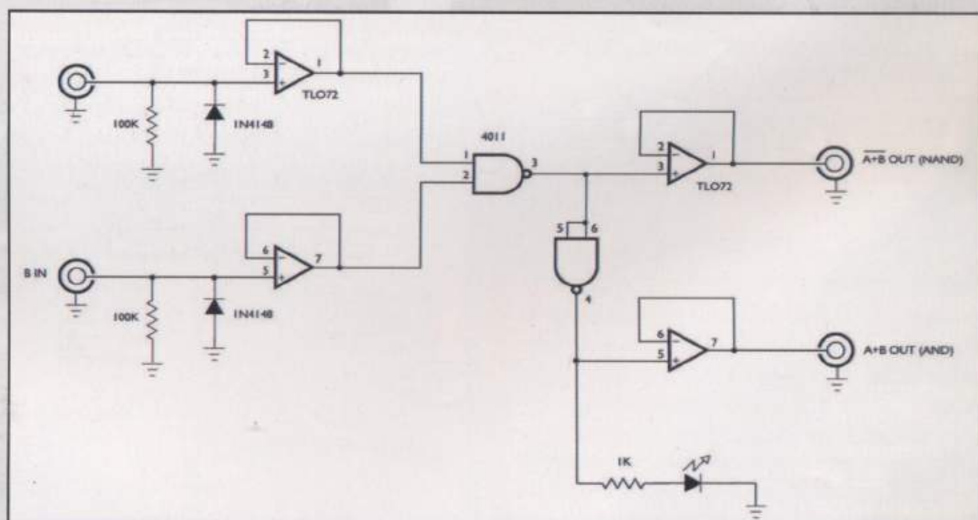
Gli apparecchi IMSI-Catcher nascono con lo scopo di determinare l'identità dei telefoni che si trovano attorno a lui, ma la maggior parte è anche in grado di ascoltare le chiamate. L'identità del telefono è formata dal codice International Mobile Subscriber Identity (IMSI), associato alla SIM del telefono, e dall'International Mobile Equipment Identifier (IMEI), che è praticamente un numero di serie del telefono. Gli IMSI-Catcher consentono di praticare un tipico attacco man-in-the-middle: il cellulare usa senza saperlo l'apparecchio al posto della normale antenna di cella e gli invia la trasmissione della chiamata. L'IMSI-Catcher determina l'identità del telefono ed eventualmente può essere usato per togliere o indebolire la cifratura, prima di inoltrare la chiamata alla sua destinazione naturale. Qualunque azienda con esperienza nella fabbricazione di apparecchi per il collaudo delle reti GSM può fabbricare un IMSI-Catcher.

Tutti abbiamo in casa un computer. Ma quanti di noi sanno effettivamente cosa succede a livello del singolo bit quando schiacciamo il pulsante di accensione?



PC: PER USARLO BENE

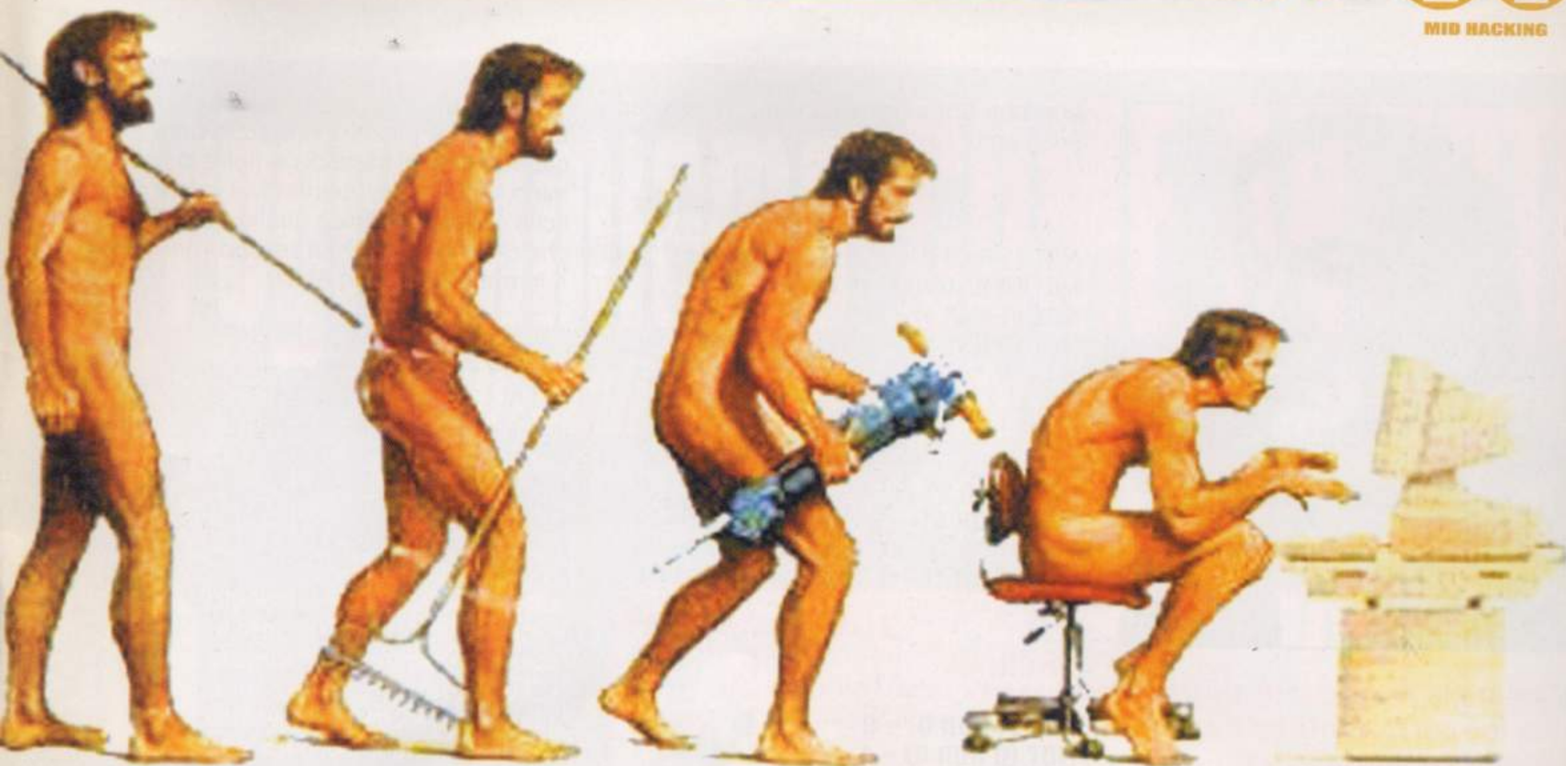
Per capire come funziona un computer, dobbiamo partire dalla sua base. Che cos'è un bit. Si sente tanto parlare di bit, megabit, gigabit… e molti di noi ancora si chiedono: cos'è, questo fantomatico bit? Bene, è presto detto: il bit è un impulso. Un minuscolo impulso elettrico che viaggia sui circuiti integrati della nostra "scatola magica". Può assumere due diversi valori, 1 o 0, oppure true o false, vero o falso, o una qualsiasi altra coppia di valori che si escludano a vicenda (ad esempio nero o bianco). Il concetto del bit, però, è solo una semplificazione che l'uomo effettua per capire di cosa si sta parlando. La macchina, in sé, riconosce solo gli impulsi, i segnali. Contatto aperto, o contatto chiuso. 1 o 0. Punto. Stop. Fine. Dobbiamo abituarci, se vogliamo imparare come funziona intimamente un computer, a pensare come lui. A saper interpretare al volo il significato di 1 e 0.



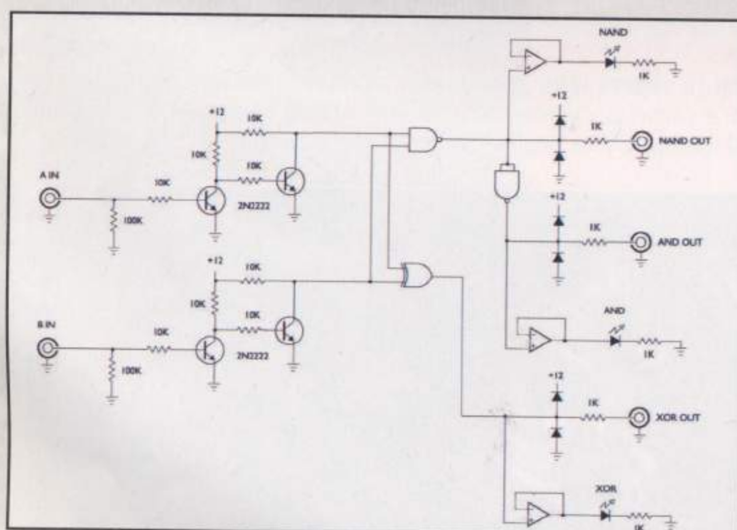
▲ *Lo schema dei circuiti elettronici che formano una porta NAND.*

Non spiegheremo dettagliatamente il funzionamento fisico della macchina, perché ci vogliono basi molto solide, soprattutto in elettronica, che non tutti potremmo avere, per capire come effettivamente un componente di un circuito integrato riesca a funzionare. Inizieremo invece a spiegare dal livello appena superiore, quello dei componenti.

In linea di massima, in un circuito integrato, troveremo un numero piuttosto



BISOGNA CONOSCERLO



▲ *Una porta NAND e altre del tipo che abbiamo descritto nell'articolo, così come si costruiscono con circuiti elettrici.*

limitato di componenti base. In particolare sono molto frequenti i componenti AND, NOT, OR e XOR. Questi “componenti”, si chiamano porte logiche, e sono alla base di qualsiasi altro componente. Le combinazioni di questi elementi, creano altri componenti, via via più complessi, fino a dare apparente vita autonoma alla nostra “scatola”. Un esempio? Se mettiamo insieme un NOT e un OR avremo un NOR, e se uniamo un NOT e un AND avremo un NAND. Le porte logiche sono equivalenti fisici degli elementi della logica booleana. Non per niente i loro nomi sono quelli delle parole che caratterizzano la logica booleana stessa. Facciamo un breve ripasso.

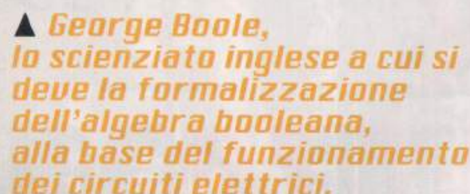
AND

Un AND è una porta logica con due entrate ed un'uscita da cui transitano i segnali. Restituisce in uscita un 1 quando entrambi i segnali in entrata sono impostati a 1.
Nello schema qui sotto e in quelli che seguono i due numeri uniti dall'istruzione AND sono quelli in entrata e il numero dopo il segno di uguale è il risultato in uscita:

1 AND 0 = 0
0 AND 0 = 0
1 AND 1 = 1
0 AND 1 = 0

OR

Un OR è una porta logica con due entrate ed un'uscita. Restituisce in uscita un 1 quando almeno uno dei due ingressi è impostato ad 1.



▲ *George Boole, lo scienziato inglese a cui si deve la formalizzazione dell'algebra booleana, alla base del funzionamento dei circuiti elettrici.*

1 OR 0 = 1
0 OR 0 = 0
1 OR 1 = 1
0 OR 1 = 1

NOT

Un NOT è una porta logica che inverte il segnale, con una sola entrata ed una sola uscita. Restituisce in uscita un 1 nel caso l'ingresso sia settato a zero, e viceversa.

NOT 1 = 0
NOT 0 = 1

XOR

Uno XOR è una porta logica con due entrate ed un'uscita.
Restituisce in uscita un 1 quando i due ingressi sono diversi.

1 XOR 0 = 1
0 XOR 0 = 0
1 XOR 1 = 0
0 XOR 1 = 1

Ora proviamo a combinare le porte logiche che abbiamo visto fino ad ora, ed otterremo:

NAND:

NOT (1 AND 0) = 1
NOT (0 AND 0) = 1
NOT (1 AND 1) = 0
NOT (0 AND 1) = 1

NOR:

NOT (1 OR 0) = 0
NOT (0 OR 0) = 1
NOT (1 OR 1) = 0
NOT (0 OR 1) = 0



XNOR:

NOT (1 XOR 0) = 0
NOT (0 XOR 0) = 1
NOT (1 XOR 1) = 1
NOT (0 XOR 1) = 0

Il concetto non è difficile, ora proviamo a complicare un po' le cose. Colleghiamo insieme alcuni di questi componenti. Ad esempio, colleghiamo due AND alle due entrate di uno XOR.
Chiameremo le 4 entrate dei due AND rispettivamente 1A, 2A e 1B, 2B. Chiameremo quindi le entrate dello XOR (che sono poi le uscite dei due AND) 1C e 2C.
Ed ecco un piccolo esercizio utile per capire bene: si tratta di riempire lo schemino sottostante, riportando il valore d'uscita del circuito (cioè quello dello XOR, che chiameremo EX) a seconda dei valori in entrata dei due AND.

1A	2A	1B	2B	1C	2C	EX
0	0	0	0			
0	0	0	1			
0	0	1	1			
0	1	0	0			
0	1	0	1			
0	1	1	1			
1	0	0	0			
1	0	0	1			
1	0	1	1			
1	1	0	0			
1	1	0	1			
1	1	1	0			
1	1	1	1			

Sembra difficile? Niente panico. Rileggendo il comportamento delle porte logiche elementari in realtà non è così laborioso rispondere esattamente. Come faremo in un prossimo articolo. :-)

Giacomo Rizzo - Alt[0]s

LOGICA DA WEB

È possibile informarsi (e sapere tutto sulla logica booleana) anche collegandosi a http://www.google.it e cercando "logica booleana" o "algebra booleana" o "algebra di Boole" nel Web di lingua italiana. Chi sa l'inglese può cercare "boolean logic" su Google.com.

Programmiamo COME ARTISTI

Il codice "offuscato" lo scrivono i geni, ma ci si divertono tutti

Obfuscated code, o codice offuscato: è l'arte di scrivere programmi disponendo il codice a mostrare un disegno. E il codice deve funzionare comunque! Meglio ancora se l'algoritmo è nascosto dentro il codice, difficile

```
123456789012345678901
234567890123456789012
345678901234567890123
456789012345678901234
567890123456789012345
678901234567890123456
```

da individuare. Scrivere codice "offuscato" non è da tutti. Ma tutti però possono provare. Chi vuole cimentarsi, mi scriva: sarà pubblicato! Nel frattempo, ecco una galleria di qualche gioiello dell'obfuscation.

Michele Campovecchio
michele_c@hackerjournal.it

CALCOLO ALLA RADICE

Questo programma in linguaggio C (http://www.bme.jhu.edu/~rcheong/) calcola la radice quadrata di un intero. A guardarlo c'è anche un indizio... :-)

```
#include <stdio.h>
int l;int main(int o,char **O,
int I){char c,*D=O[1];if(o>0){
for(l=0;D[l              ];D[l
++]-=10){D   [l++]-=120;D[l]-=
110;while    (!main(0,O,l))D[l]
+=   20;   putchar((D[l]+1032)
/20   )    ;}putchar(10);}else{
c=o+       (D[I]+82)%10-(I>l/2)*
(D[I-l+I]+72)/10-9;D[I]+=I<0?0
:!(o=main(c/10,O,I-1))*((c+999
)%10-(D[I]+92)%10);}return o;}
```

PALLE, PALLE, PALLE

Questo programma Perl (http://www.perlmonks.org/index.pl?node_id=339774) fa in 3D ciò che mostra nella sua forma ASCII:

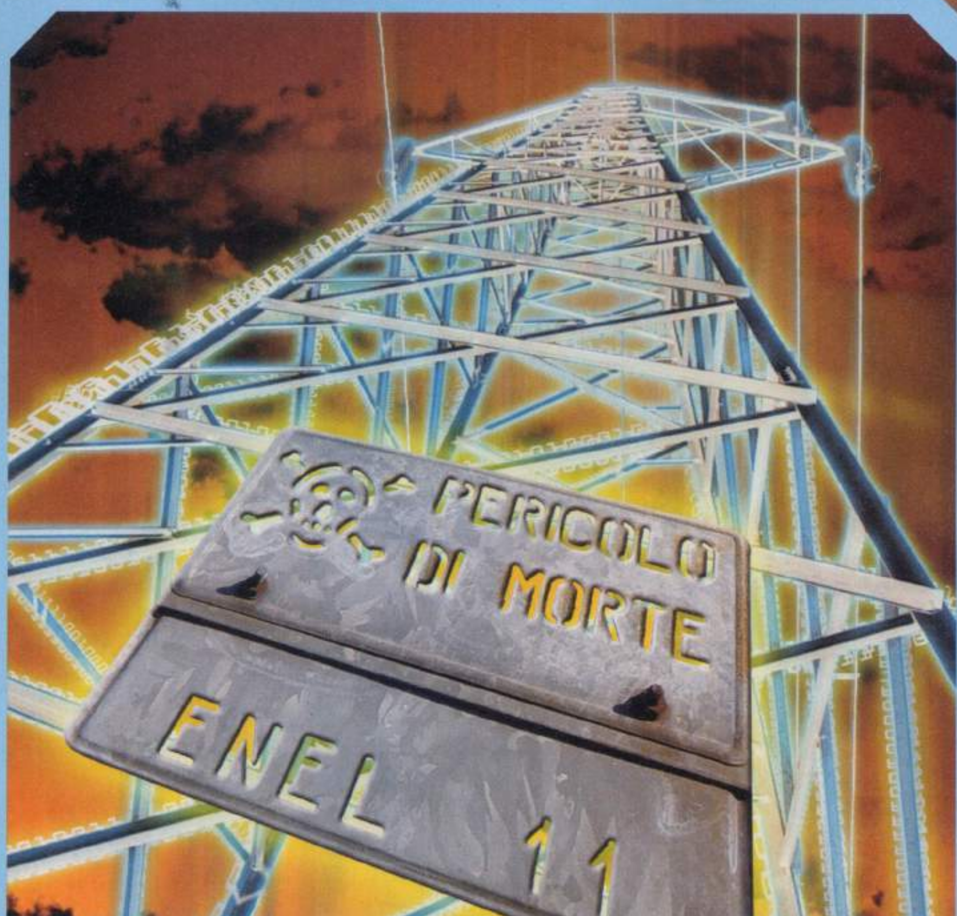
```
     $_=q%$_="                   88GGCI";
   @a=/./g;@_=('IP            ""YI','IjjjjI',
   'IiciII')    ;whil        e($c=pop@   a){ma
  p{$_=$c.$_    .$c}@_      ;@_=(($t=(   $n=$a[
 $#a]||"@").$     {c}x(-   2+length$_[0]).$n),@_,
 $t)}$_='j8_4xj4,@@8b,x    j2,@14bxjd@16bxd@18bx@
 20x@20x@20xY@18PxjY@16    Pxj`Y@14Pxj4`@10Pxj8"5
 x';s#(.)(\d*)#$1x($2||    1)#eg;$m=2;$n=-1;$|=1;
  $p=9;$q=20;{$q+=$n*=      $q<11|$q>50?-1:1;$p+
   =$m*=$p<8|$p>16?-1        :1;$u=-$q*6/($l=($
     q**2+$p**2)**.5           );$v=-2-$p*6/$l;
       $r=$p-6;$                  s=$q-9;$y=0
                   ;select$x
                 ,$x,$x,.2*print
                "\ec*",(m   ap{$l
                =0;"\e[".$     r++.";
               ${s}H",$y++<$v?$_:do{@
               c=split//,$_[$y-$v-1];
               map{$l++>$u&/@/&&($t=$
               c[$l-$u-2])?$t:$_}/./g
                },$/}splitjx),"\e[30
                 H";redo}%;s#\s##g;
                   s#j#$"#g;eval
```

L'ORA DEL DROMEDARIO

Un orologio o una nave del deserto? Mah. http://perlmonks.thepen.com/190308.htm

```
#!perl  -w
 use strict;
 $_='
           $,=$/;$|=@_
        =split//,"Justan                       othe
    rPerl.hacker";$/=\'$?~=                (local  tim
  e)[$.]*($.==0||$.==1??1:5);s           ubstr($_,eval
\\\'$^=$-*2*atan2(1,?1)/15;int(-  cos($^) *($=+
1)+11.5)*25+int(sin(?$^)*($=+1)+12.5)\\\'?,1,
$_[$=+(11,4,0)[$.]])?\';do($_=(".*x287).
"#"."."x287;for$=(0.?.10){$.=0;eval$/;
$=<7&&($,=1,e              val$/);$=<4&
 &($.=2,ev                  al$/);}p
   rint(p                    ack("
   c3  ",                     27,9
   1,  72                     ),(/
   .(  25                     )/g)
   ,s  ca                     lar(
   lo   cal                   time)
   );}   whil                 e(slee

p(1))';s/\s+//g;eval
```



PC e

Noi vogliamo tenere sempre acceso il nostro PC. Vogliamo essere sempre in contatto col mondo. Magari per tenere sempre sotto controllo la posta elettronica. Nostra madre ci urla di spegnere perché consuma corrente. Ma quanto consuma il nostro computer?

PERICOLO DI MORTE!

Facciamo attenzione a montare il circuito che abbiamo descritto. Montiamolo quando il cavo è staccato da tutto, avvolgiamo parecchio nastro isolante intorno ai morsetti e a tutti i fili scoperti, non tocchiamo mai e poi mai nemmeno inavvertitamente la resistenza o i puntali scoperti del tester. Quando attacchiamo il cavo al computer e alla presa di corrente, non lasciamolo mai incustodito e usiamolo solo per il tempo strettamente necessario alla misura. Poi rimettiamo il cavo originale. Non tocchiamo mai la resistenza, nemmeno per vedere 'se scalda'. A parte il fatto che non scalda, dobbiamo assolutamente evitare di venire in contatto con qualunque parte dove passano i 230 Volt che ci fornisce l'Enel. Sono mortali!



Se guardiamo il catalogo prodotti all'indirizzo www.dmail.it, scopriamo un 'Misuratore del consumo di energia elettrica' che inserito tra la presa e la spina dei nostri apparecchi consente di vedere quanto consumiamo in corrente elettrica. E fa perfino i conti per noi: è sufficiente che gli inseriamo la tariffa dell'Enel, approssimativa, e leggiamo la cifra su display digitale. Carino, utile, preciso e sofisticato: ci costerà 39,00 Euro.

Niente di più economico?

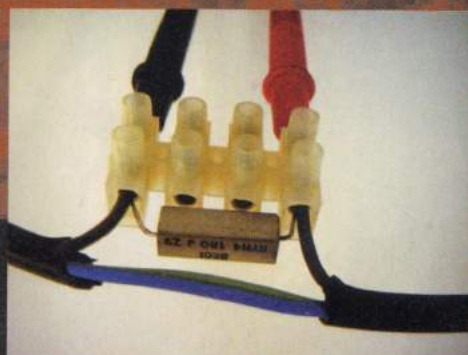
Decisi a spendere di meno, ci siamo messi a progettare un misuratore di consumi e pensandoci un po' abbiamo deci-



▲ ***Tutto il circuito:** il cavo per pc, il morsetto per tenere fissa la resistenza, il cavo di alimentazione e i puntali del tester. Un tester che misura i volt alternati.*

so di provare un metodo un po' grezzo, ma indubbiamente meno costoso. Ci siamo procurati:
Una resistenza a filo da 1 Ohm, 10 Watt

BOLLETTA ENEL



(1 Euro, circa, o recuperata da un televisore non più funzionante)
Un morsetto 'mamut' per serrare i fili (0,50 Euro circa)
Un cavo di alimentazione per computer (1,5 Euro circa)
Un vecchio tester per la sola parte di misura delle tensioni (se non l'avete, trovate qualcosa sulle bancarelle dell'usato o nei superstore a poco più di 7 Euro)
Un po' di nastro isolante (quello almeno l'abbiamo già in casa)
Se quindi proprio va male abbiamo speso 11 Euro, ma abbiamo rimediato un tester che servirà tenere in casa per altri scopi. Se abbiamo già un minimo di attrezzatura, forse dobbiamo acquistare solamente la resistenza: 1 Euro e siamo posto.

Come funziona?

Forti di qualche noiosissima lezione di elettrotecnica, abbiamo collegato la resistenza in serie a un cavo di alimentazione del computer, sistemando le cose in modo da poter collegare ai capi della resistenza anche i due puntali del tester, predisposto sulla misura dei volt.

Poi ci siamo ricordati che:
- la corrente che passa nel circuito (quindi anche nel computer), passa tutta anche attraverso la resistenza;
- se misuriamo la tensione ai capi della resistenza, questa si chiama 'caduta di tensione della resistenza' e dipende dal valore della resistenza e dalla corrente che ci scorre dentro;
- con una divisione e una moltiplicazione, usando della legge di Ohm, ricaviamo la potenza che ci interessa e, se proprio vogliamo sapere cosa costa, ci servirà una bolletta dell'Enel da cui ricavare il prezzo del Kilowattora.

Ecco cosa è successo

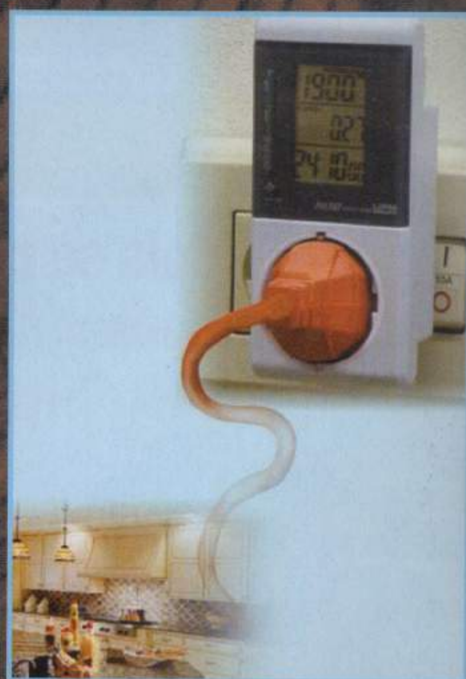
Dunque, la legge di Ohm è semplicissima e dice che Corrente (in Ampere) = Tensione (in Volt) / Resistenza (in Ohm). Ma stiamo usando una resistenza da 1 Ohm, quindi a noi risulta Ampere = Volt/1
Attaccando il tester ai capi della resistenza, leggiamo esattamente i Volt, ma il valore che leggiamo, nel nostro caso, è quindi uguale al valore della corrente elettrica che sta passando nella resistenza, in Ampere.



Facciamo finta di leggere sul tester 0,400 V. Equivalgono a 0,400 A. Benone! Ci manca solo una moltiplicazione.
La potenza, in Watt, si calcola infatti sapendo gli ampere e i volt, con la formuletta Potenza (in Watt) = Tensione (in Volt) x Corrente (in Ampere).
Niente di più semplice, vero? Ma attenzione, qui la tensione in volt è quella che abbiamo applicato al circuito nel suo complesso, quindi al computer alimentato dal nostro cavo. Ovvero la pericolosa tensione della rete elettrica, che in Italia è, da qualche tempo, 230 Volt alternati. Facciamo i conti: Potenza = 230 V x 0,400 A = 92 W.
Ecco fatto, sappiamo quanto consuma il nostro PC: meno di una lampadina da 100 W.

E quanto spendiamo? Dipende, perché il calcolo che fa l'Enel sulle bollette è complicatissimo e dipende da quanto consumiamo nell'arco di tutto l'anno. Ma approssimativamente, facciamo come se per ogni mille Watt consumati ogni ora pagassimo 0,26 Euro, o giù di lì.
Quindi, se teniamo acceso il nostro PC un'ora, consumiamo 0,092 KW, ovvero poco più di 2 centesimi di Euro all'ora; 0,57 Euro al giorno, poco più o poco meno. Meno di un caffè.

Standard Bus
standardbus@softhome.net



È ARRIVATA LA RIVISTA PER I WEBMASTER



Webmaster Journal è la rivista che ci dà quello che serve per creare un sito internet da zero e metterlo in rete in pochissimo tempo. Tratta in modo semplice e immediato tutti i temi caldi del Web, dalla progettazione delle pagine ai problemi più comuni di programmazione e realizzazione. L'approccio è estremamente pratico e quello che viene spiegato può essere impiegato subito apportando delle semplici modifiche alle pagine che vengono incluse sul CD. Inoltre, sul primo numero si trova in regalo Xara WebStyle 2, un programma completo che crea in pochi clic tutti gli elementi grafici di cui un buon sito ha bisogno: dai banner ai pulsanti animati, passando per divisori, loghi e menu. Sul CD si trovano anche delle raccolta di template gratuiti per pagine web e moltissimi programmi che rendono più facile la vita di chi lavora con Internet. Abbiamo programmi per creare siti web, client FTP, gestori del download, utility che realizzano filmati in flash partendo solo da uno slogan di testo e anche l'immancabile antivirus. Infine, una rubrica curata da un esperto risolve i piccoli intoppi che ogni giorno si presentano al webmaster. Insomma, una guida semplice e immediata a una delle professioni più affascinanti della nuova era informatica.



LA GUIDA PRATICA CON IL SOFTWARE PER FARE SITI INTERNET

Ritaglia lungo la linea tratteggiata

BUONO SCONTO

Solo se compilato in ogni sua parte, **consegnandolo** al tuo edicolante avrai **diritto** allo **sconto di € 0,50**

Vale 0,50 €

UTILIZZO IL BUONO SCONTO PER IL:

NUMERO 1 ❒

NUMERO 2 ❒

Cognome ....

Nome ....

via ....

CAP .... CITTÀ .... PR..........

Firma ....

E-mail ....

4ever

Potrai pagare la tua copia della rivista solo € 4,49. La 4ever S.r.l attraverso il suo distributore Parrini & C. S.p.A. girerà lo sconto di € 0,50 per l'acquisto di una copia della rivista *Webmaster Journal* agli edicolanti che consegneranno questo buono ai distributori locali. Il presente buono scadrà il 31/05/2004.

Timbro Edicolante

Comunicazione importante: La 4Ever Srl – Via Torino 51, 20063 Cernusco s/N (MI) – titolare del trattamento, raccoglie presso di Lei e successivamente tratta, con modalità anche automatizzate, i Suoi dati personali per la gestione dell'abbonamento e, se lo desidera, per l'invio di informazioni commerciali su prodotti e servizi della 4Ever Srl. Il conferimento dei Suoi dati personali è facoltativo, ma serve per l'esecuzione dei servizi sopra indicati. È designata Responsabile del trattamento Staff srl – Via Bodoni 24, 20090 Buccinasco (MI). Lei può esercitare in ogni momento i diritti di cui al DL 196/2003 (accesso, correzione, integrazione, opposizione, ecc.) rivolgendosi alla 4Ever Srl, titolare del trattamento dei dati.